



Data Protection Commissioner

An Coimisinéir Cosanta Sonraí

Fourteenth Annual Report of the Data Protection Commissioner

2002

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

PRN. 79

CONTENTS

Foreword	3
Réamhrá	5
Part 1 - Activities in 2002	
Introduction	8
Promoting Public Awareness	8
Enquiries	11
Complaints	12
The Public Register	14
Legislative Development	16
International Activities	17
Administration	21
Part 2 - Case Studies	
Motor Insurance	24
Phone recording by bank	24
Gardaí "Pulse" system	26
Canvassing at elections and phone marketing	27
Journalist's phone calls	29
Women's Mini Marathon	30
Spanish apartment purchase	31
Army Deafness	32
Bank Security breached	35
Aer Rianta and PPSN	36
Chemists and infectious diseases	37
Appendices	
Appendix 1 Communications Traffic Data	40
Appendix 2 Public Awareness Survey	45
Appendix 3 Health Unique Identifier Number	50
Appendix 4 Strategy Statement	52
Appendix 5 Financial Statement	60
Appendix 6 Registrations by Sector 2000-2002	61

FOREWORD

I am pleased to present the fourteenth Annual Report in relation to the work of the Office of the Data Protection Commissioner since it was established in 1989. It outlines the activities of my Office during 2002.



In the current information era the concepts of privacy and data protection are on occasions put forward as a barrier to progress. On the contrary I feel strongly that for the information society to succeed it is vital that good data protection practices are in place. Improved levels of service, identification, anti-fraud measures, surveillance actions to prevent and investigate crime- including cybercrime-and terrorism are significant concerns in the modern global world. While we all can accept the need for many of these initiatives there is, however, a real danger that the human right to privacy can be overlooked or indeed diminished by some of these demands if a proper balance is not struck. Accordingly, if we are being asked to sacrifice our privacy rights we must have details about what we get in return. Once privacy rights are surrendered they may be hard to recover. We should therefore surrender these rights reluctantly, on the basis of convincing arguments and facts about other interests of society which need to be balanced. Legislators, accordingly, have a responsibility to debate these matters in an open and frank manner.

I believe it appropriate to reiterate in this Report to the Oireachtas that I am also conscious of the sensitive issues of crime and security, including national security. As Data Protection Commissioner, I will be supportive of measures that are demonstrably necessary to protect against crime or terrorism but such measures must be proportionate and have regard to the human right to privacy.

During 2002 I continued the dialogue, begun in late 2001, with the Department of Justice, Equality and Law Reform regarding what I considered as disproportionate the retention period, for security purposes, of communications traffic data. I am pleased that the matter became the subject of public debate during 2003. For such traffic data to be retained in specific cases for security purposes, there must be a demonstrable need, the period of retention must be as short as possible and the practice must be clearly regulated by law, in a way that provides sufficient safeguards against unlawful access and any other abuse. (Appendix 1 refers)

The results of the public awareness survey carried out for my Office and outlined later in the Report are indications of the fears that many people have about their privacy rights being undermined. Major implications, accordingly, arise for eCommerce and eGovernment, as their success will ultimately depend on public credibility. The survey also poses major challenges for me and a public awareness strategy is, accordingly, being devised for the coming year. (Appendix 2 refers)

The Personal Public Service Number (PPSN) was introduced in the 1998 Social Welfare Act as the unique personal identifier for transactions between individuals and Government Departments and other agencies specified in the Social Welfare Acts. I commend the Department of Social and Family Affairs for launching a code of practice and a publicity campaign during 2002 as to what the PPSN really is. It is not a national identifier number and it cannot be used in the commercial world though where instances have been brought to my attention on occasions I have ensured that this practice ceased. While the Department of Health and Children have considered applying it as a unique health identifier number for the health sector my concerns with this proposal are outlined in detail in Appendix 3.

On a positive note the Irish Internet Association (<http://www.ia.ie>) are to be complimented for devising, with co-operation from my Office, a template for privacy statements to be carried on its members' web sites. This "public / private partnership" is an indication that business is aware of the competitive advantage it can enjoy if it clearly indicates how personal data is collected and used. I hope its members will implement it during the coming year. I look forward to similar developments of co-operation from other parties particularly when codes of practice are being devised because I want to have a participative approach to my role. I am also pleased to compliment the progress being made by GPs and the GPIT unit of the Department of Health and Children (<http://www.gpit.ie>) in collaboration with my Office in drawing up such a code for GPs.

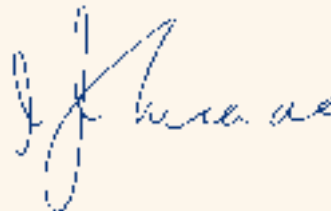
The expected transposition of the 1995 EU Data Protection Directive into Irish law did not materialise during 2002 as the Data Protection (Amendment) Bill,

2002, though initiated in February 2002, was not enacted until April 2003. It will become operational during 2003. However provisions in the Directive regarding transfers to non-EEA countries and security of personal data took effect from April 2002. The transposition of the 1997 Telecommunications Directive took effect from May 2002. Giving effect to these Directives will be a major part of my Office's work in the coming year.

The year was a very busy one for the Office overall with increased levels of activity in all areas. I am indebted to my office staff for once again ensuring that a valuable public service has been provided overall in a timely, fair and efficient manner. In this regard, a new Strategy Statement produced in February 2003 (Appendix 4) takes account of our increased role and responsibilities. Extra resources given to me over the last two years has enabled the Office to carry out much needed work and to streamline procedures. As Data Protection law is now quite complex I will keep the resource situation under review because I am constantly aiming to improve the level of service that people and organisations rightly demand from my Office and me.

I am grateful to the many people who contacted my Office and brought serious matters to notice. I also thank the majority of data controllers who generally complied fully with the law as well as the Minister for Justice, Equality and Law Reform and his officials for support and the continuing good relations between our Offices.

Finally I look forward to a fuller recognition of the value of Data Protection in every day life and that it is seen not only as an enabler but as a means of empowering people to protect their human right to privacy.



Joe Meade
Data Protection Commissioner

16 April 2003

Réamhrá

Is mian liom a chur i láthair an ceathrú Tuarascáil Bliantúil déag i leith obair Oifig an Choimisinéir Cosanta Sonraí ó bunaíodh é sa bhliain 1989. Cuireann sé síos go mion ar gníomhaíochtaí mo Oifig i rith na bliana 2002.

Sa ré faisnéise atá ann i láthair na huairé cuirtear ar uairibh coincheap an phríobháideacais agus cosaint sonraí chun tosaigh mar bhac ar dhul chun chinn. Ar an dtaoibh eile de, táim féin den tuairim láidir go bhfuil sé riactanach chun go neireódh leis an sochaí faisnéise go gcurfí cleachtaithe maithe cosant sonraí i bhfeidhim. Leibhéal feabhsaithe seirbhíse, aitheantais, modhanna frith calaoise, gníomhaíochtaí, airdeallachia chun cosg a chur ar choiriúlachta-coiriúlacht cibear san áireamh-agus sceimhlitheoiracht agus iad a fhiosrú, cuirtear iad san chun chinn mar riachtanas i gcursaí domhanda an lae inniu. Biodh is gur féidir linn glacadh le riachtanas a lán de na tionscnaimh seo, tá ,mar sin féin, baol suntasach go ndéanfar an ceart daonna do phríobháideachas a ligint i ndearmad nó laghdaithe ar cuma ar bith ag cuid do na héilimh sin muna ndéantar cothraimíocht ceart ar na chúrsaí seo. Dá bhri sin, má táthar ag iarraidh orainn ár gcearta príobháideacha a íobairt, caithimid sonraí - firicí agus figúirí - a fháil faoi cad a gheobhaimid ina chúiteamh sin. Nuair a scaoiltear le cearta príobháideachais, bíonn sé rí dheacair iad a fháil thar nais. Ba chóir dúinn mar sin na cearta sin a scaoileadh uainn go drogallach, ar bonn argóintí eifeachtacha agus na firicí i dtaoibh spéiseanna eile an chomhluidair. Tá freagaracht mar sin ar reachtóirí na nithe seo a phlé i modh oscailte macánta.

Creidim gur chóir dom a athlua sa Tuarascáil seo don Oireachtas go naithním freisin go bhfuil ábhar íogaracha i dtaoibh coiriúlacht agus slándálacht, go háirithe slándálacht náisiúnta, i gceist. Mar Choimisinéir Cosaint Sonraí, tabharfidh mé tacaíocht do mhodhanna atá riactanach go soiléir mar chosaint i naghaidh coiriúlacht nó sceimhlitheoiracht ach caithfidh na modhanna sin a bheith comhréireach agus aird a bheith ann don ceart daonna do phríobháideachas.



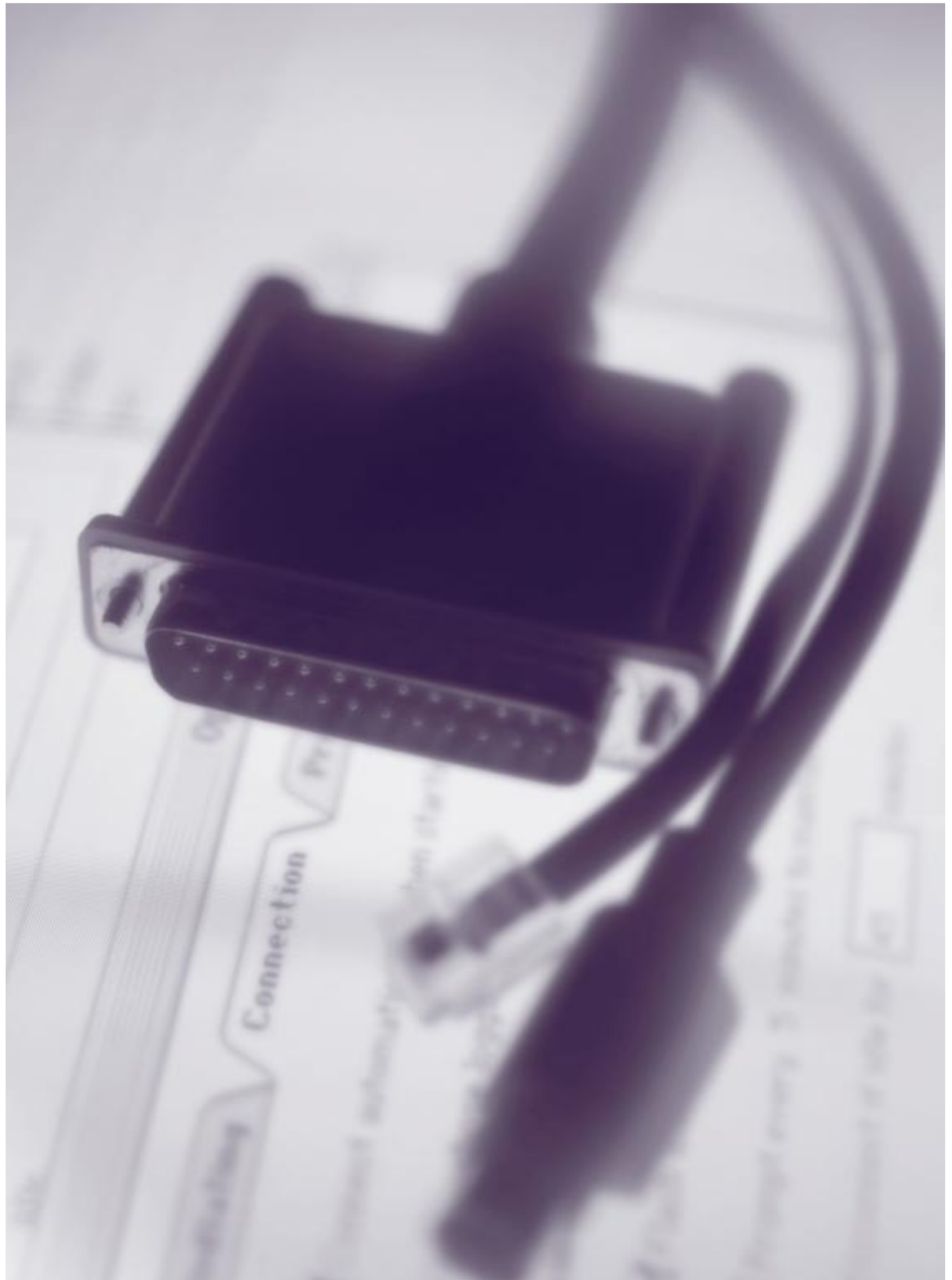
Léiríonn torthaí an suirbhé eolas poiblí a cuireadh i gcrích don Oifig seo, agus a rianófar níos faide ar aghaidh sa Tuarascáil, an fhaitíos atá ar a lán daoine go ndéanfar a cearta daonna a lagú. Tá impleachtaí tromcúiseacha dá bharr do e trachtáil agus e riaracháin mar braithfidh a rath sin sa deireadh ar creidiúint poiblí. Ardaíonn an suirbhé seo dubhshláin móra dom féin agus mar sin tá straitéis eolais poiblí a leagann amach don bhliain atá romhainn.

Tá mé buíoch don na daoine go léir a chuaigh i dteagmháil le mo Oifig agus a thóg nithe tromcúiseacha chun aird. Tugaim buíochas leis do fhormhór rialaitheoirí sonraí a choimhlon tríd is trí go hiomlán an dlí agus mo bhuíochas don Aire Dlí agus Cirt, Comhionannais agus Athcóirithe Dlí agus a chuid oifigigh as ucht an tacaíocht agus an caidreamh leanúnach maith idir na hOifigí againne.

Ar deireadh, tá mé go mór faoi chomaoin ag mo fhoireann oifige gur dheimhin siad deimhin de arís, i dtoscaí an deacair ar fad, seirbhís fiúntach poiblí a chur ar fáil tríd is tríd i modh tráthúil, cothrom agus éifeachtach.

Seosamh Ó Midheach
Coimisinéir Cosanta Sonraí

16 Aibreán 2003.



Connection

Pre

Connect automatically when start

every 3 minutes to see

of size for []



Part One
Activities in
2002

Part One Activities in 2002

Personal data about individuals is collected and used as part of every-day life by organisations (Data Controllers) that provide goods and services in both the public and private sectors. The ease and speed with which personal data can be processed and transmitted over computer and telecommunications networks has increased greatly in the last decade, particularly in the case of the rapid development of the Internet. This has brought about great benefits for society and for people who are able to conduct personal and business matters conveniently and quickly. At the same time, Governments and Business want to be able to share information in order to provide better and more efficient and integrated services.

This is the context within which Data Protection Law (the Data Protection Acts 1988 and 2003) provides a legal framework for the protection of peoples' personal data. It imposes responsibilities and obligations on Data Controllers and gives rights to Data Subjects. The Office of the Data Protection Commissioner is responsible for enforcing this body of Law. This involves a wide range of statutory functions, both in Ireland and at European level, relating to the promotion of awareness of Data Protection amongst Data Controllers and the public, the investigation of complaints, the maintenance of the Public Register and liaison with international authorities. This section describes the main activities of my Office in these areas in 2002, with particular focus upon a number of matters that I consider to be of particular interest.

Promoting Public Awareness

Data protection is sometimes characterised as being about technology or about the law. In fact, although it relates to both, it is more fundamentally about the application of good principles of information management of personal data. The key principle is that personal data belongs to the individual data subject and people should be able to control how others use such information about them - or at the very least to know how the information is used.

Developing public awareness and appreciation of the existence of Data Protection rights and how they are enforced is a key function of the Office. During recent years, we have concentrated our resources on liaising with the larger Data Controllers in the public and private sectors that control data on tens of thousands of data subjects. By seeking to ensure that these Data Controllers adhere to Data Protection requirements, we are directly contributing to the protection of the rights of their data subjects. While we have not to date carried out focussed campaigns aimed at the general public, the results of the Awareness Study detailed in Appendix 2 show that, at the broadest level, they are keenly aware of the importance of privacy in relation to their personal information. With the enactment of the new legislation in April 2003, I will need to complement our existing Information and Awareness strategies with focussed publicity - using locally based print and broadcast media - aimed at the general public around the country.

During the year, I pursued the promotion of public awareness in the following principal ways:

- Publication of information booklets
- Website information
- Media advertising
- Direct contacts – e.g. talks and presentations to groups, and participation in working groups and fora.

Information booklets

My Office makes available to the public, free of charge, a range of explanatory leaflets and booklets on Data Protection. In 2002, my Office distributed approximately 20,000 such leaflets to organisations and members of the public. This shows a steady level of demand compared with the previous year. The booklets are being completely revised and up-dated to give comprehensive information on the changes in the Data Protection (Amendment) Act, 2003. I urge all Data Controllers and Data Subjects to familiarise themselves with these changes by reading these

Part One - **Activities in 2002**

booklets for themselves. I also expect that the publicity campaign which my Office intends to launch to coincide with the coming into operation of the Act will give rise to an increased demand for clear and concise explanatory material. The Booklets, which will be available from my Office, will be

- Data Controller's Guidance booklet.
- Data Subject's Guidance booklet.
- What's new in the Amendment Act - a Summary Guide.
- Data Controller's Registration requirements.

Website information

The Office Website has been an outstanding success, reducing, as it has, the number of basic routine queries received by the Office. In 2002, there were 20,000 visitors to the Site and the feedback that we have received is that most people have found it to be useful and informative. However, it is not a substitute for the printed leaflets or telephone contact - rather, it complements them and gives visitors more detailed and specialised information and guidance. Keeping the Website up to date poses a constant challenge for my Staff, given the extent of change in Data Protection Law in the last year (see Legislative developments below). However, I am committed to respond to this and allocate sufficient resources to its up-dating so that the quality and range of information available is appropriate to the needs of Data Controllers and Data Subjects. The provision of up to date and accurate Guidance on the Web Site is crucial to our overall Mission of empowering Data Subjects.

During the coming year, it is my intention to further develop the Website and investigate the possibility and feasibility of providing on-line access to the Public Register of Data Controllers and Data Processors and also of providing for on-line processing of applications for registration. I would encourage the public to visit www.dataprivacy.ie to see for themselves the range of useful information, and indeed to offer suggestions for improvement.

Media advertising

During 2002, expenditure on media advertising totalled €45,000. This involved a continuation of the strategy of previous years of placing data protection advertising in a range of publications aimed at both the public in general and data controllers responsible for handling personal data.

The cost of the Awareness study carried out was €14,000. The Study is important for the Office as it illustrates areas where awareness is low and focus is needed and it also provides a Benchmark from which we plan to "grow" awareness. Having regard to the findings and the need to disseminate information on the new Act, I intend to reactivate our Education and Awareness activities in the coming year, utilising a range of locally based print and broadcast media.

Direct contacts

Talks and presentations

The information channels outlined above are vital to the spread of information about Data Protection. It is important also that we win the attention of those with responsibility for Governance in organisations and, as such, there is no substitute for direct contact by the Office with Data Controllers. In this way, it is possible for the Office to explain the details and nuances of Data Protection law while, at the same time, hearing about the practical issues that face Data Controllers on the ground. The resulting exchanges make for better understanding of the reasoning behind our Guidance but it also creates an opportunity for my Staff to take on board legitimate concerns that will not take away or diminish protection of Data Subjects. In 2002, my Staff and I delivered presentations to a wide range of groups, of which the following are a representative sample:

■ **Financial Institutions**

I engaged in discussions with a number of major financial institutions which were anxious to ensure maximum compliance with Data Protection rules.

Part One - **Activities in 2002**

■ **Information Society Commission**

I made a presentation to the Commission emphasising that respect for Data Protection and privacy would enhance the trust of citizens in eGovernment and eCommerce, thereby contributing to the success of Information Society initiatives.

■ **Health Boards / Health Authorities**

My Office engaged in discussions with the Department of Health and Children and a number of Health authorities in 2002 on the issue of Data Protection in Health Care. Amongst the matters addressed were the drafting of a Code of Practice for General Practitioners governing the use of personal data in General Practice. The application of Data Protection Law in Hospitals and Health Authorities and the issues posed by medical research were also considered. A major focus was the proposed use of the PPSN as a unique identifier for Health Records as outlined in Appendix 3.

■ **Government Departments**

My staff made a number of presentations to Government Departments on Data Protection obligations, referring, amongst other matters, to the respective roles of Data Protection and Freedom of Information in so far as access to personal data is concerned.

■ **Credit Referencing**

I made a presentation to the annual Meeting of the Irish Credit Bureau that provides a credit referencing service to Financial Institutions. The principal point of the talk was the importance of clear consent and transparency in the process.

■ **Direct Marketing Sector**

I made two presentations to the Irish Direct Marketing Institute (IDMA) on the implications of the European Data Protection Directive for their operations in order to clarify matters relating to Data Subject consent for Direct Marketing. I anticipate that a Code of Practice for the Sector will emerge from these discussions.

■ **Irish Internet Association**

I participated in the process leading up to the launch by the Association of its Privacy Policy for Websites. This initiative of the Association, which I welcomed and support, requires Websites to clearly outline how data is collected and used.

■ **Insurance Sector**

My staff made a number of presentations in the Insurance Sector and a meeting was also held with the Insurance Federation of Ireland. The intention is that the Federation will draft a code of practice for my review setting out the application of Data Protection law in this sector.

■ **Legal firms**

I made a number of presentations at seminars organised by Legal Firms for their clients. I found these particularly useful, as I was able to engage with a large numbers of Data Controllers simultaneously on some common themes of importance.

■ **Media interviews**

Finally, I gave many media interviews at both national and local level.

WORKING GROUPS AND OTHER FORA

The Internet Advisory Board, on which my Office is represented, continued its task of seeking to encourage responsible self-regulation by the Internet service industry, with the overall aim of preventing illegal and harmful use of the Internet. I made a presentation at a major Conference organised by the Board where I underlined that Data Protection, which requires robust security and provision for consent (and parental consent where children are concerned) is a key enabler of Internet safety. The importance of parents, guardians and schools installing appropriate filtering software and the need for close supervision of children were adverted to. Further information about the Board's activities is available at its website, www.iab.ie.

My Office continued to contribute to the work of the Health Information Working Party, an ad hoc group convened by the Department of Health and Children

to advise on policy in the drafting of the National Health Information Strategy. The aim of this work is to produce an overall framework within which health information management and governance issues, including Data Protection, can be developed. A key issue in the Strategy is consideration of a unique identifier for personal Health Records (see Appendix 3).

As I made clear in recent Annual Reports, the development of computerisation in the Health Services is bringing into focus a range of health information management issues that must be addressed. I, therefore, welcome the Department's proposed National Health Information Strategy as I believe that there is a need for clarity in how medical data is handled within the health sector with clear guidelines on who can have access and in what circumstances. The key principle is that patient data should flow, as medical treatment requires, while ensuring that medical confidentiality is accorded utmost priority. Patients must know and understand how their data is going to be used and medical practitioners at every level should have clear guidance on what is and what is not legally permissible. With the publication of the Strategy, I hope that early progress can be made on the adoption of clear Codes of Practice for the health sector, building on the work already being done in the General Practitioner area by the General Practitioner Information Technology Group (GPIT), under the aegis of the Department. This is a priority for my Office.

My Office also continued discussions with the Office of the Information Commissioner and at the end of the year, discussions were taking place with a view to developing principles and guidance for practitioners and the public in the area of the overlap which exists between the two Acts in regard to access to one's own personal data /personal information which now has added importance given the extension of Data Protection to certain manual files. The Amendment Act also provides at section 1(5) that

"(a) A right conferred by this Act shall not prejudice the exercise of a right conferred by the Freedom of Information Act, 1997.

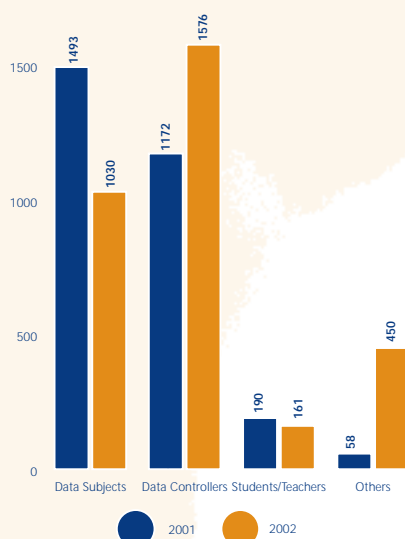
(b) The Commissioner and the Information Commissioner shall, in the performance of their functions, co-operate with and provide assistance to each other."

ENQUIRIES

The primary public service provided by my Office on a day-to-day basis is to provide information and advice as a first step to enabling people to exercise their rights. Requests for information come from individuals, from businesses and public bodies holding personal data ('Data Controllers'), and from people who may be advising others (legal professionals, teachers and citizens advice centres). With the additional resources recently assigned to me, I have allocated resources to the provision of advice and on-going staff training has been crucial to ensuring that the quality of advice provided is of a consistently high standard.

Our Website (launched in December, 2000) has made a large amount of information on Data Protection easily available, and also provides Links to European Union Data Protection Authorities as well as other sources. We find that callers are often content to check the Website and, if necessary, revert to us with more detailed queries, based on the knowledge that

Figure 1 Contacts, sorted by category

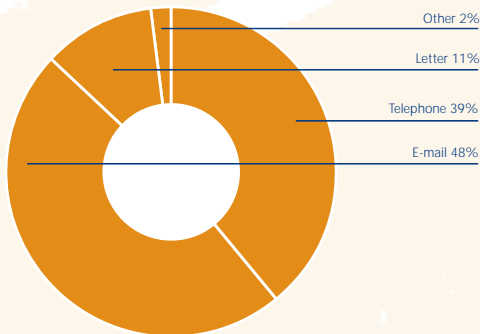


Part One - **Activities in 2002**

they have gleaned from the site. Overall during the year, the office received 3,217 enquiries compared with 2,913 in 2001. The queries have tended to be more complex, which is evidenced partly by the fact that queries from Data Controllers about their legal obligations rose from 1,172 to 1,576, an increase of 35% (see figure 1). This reflects increasing awareness amongst Data Controllers who wish to keep abreast of legislative developments in the Data Protection area. The increasing complexity of queries is posing challenges for our Staff who must be able to give clear initial advice and be able to follow this up with detailed guidance in a short time. The figure for queries from Data Controllers is encouraging as it means that our work with them is having an effect and there is, of course, a multiplier effect as Data Subjects benefit directly from the resulting appropriate protection of their data. The number of data subjects contacting the Office directly fell from 1,493 to 1,030 and while this may be due to more people accessing our Website, it is an area that I will be focussing on, as direct empowerment of individuals in relation to their Data Protection rights is a vital objective.

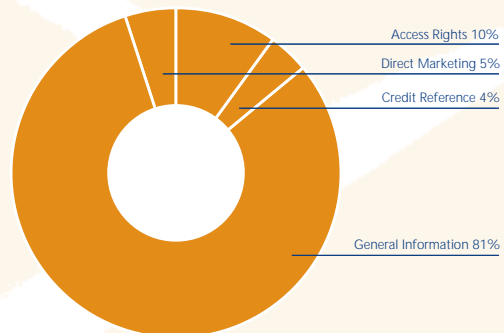
Figure 2 shows that the telephone is no longer the commonest method of contacting my Office as e-mail queries have continued to rise and now account for 48% of enquiries received. This does not, however, reflect the full extent of telephone work which remains a key method of communicating with our customers - organisations, the public and their advisers - as subsequent telephone contact about an initial issue would not be reflected in the figure.

Figure 2 Contacts, sorted by contact method



As regards the subject matter of the queries received (Figure 3) enquiries seeking General Information about, for example, obligations relating to Registration, Consent Notices, Transfers of Personal Data outside of the EEA, the rules concerning the disclosure of data to third parties and System Security Requirements accounted for 81% of contacts. Queries about access requests, checking a credit record and direct marketing were also regular. Specialist information on the compliance requirements arising from the transposition into Irish Law of the European Data Protection Directive and the Data Protection and Privacy in Telecommunications Regulations, 2002 also imposed significant workloads.

Figure 3 Data subject queries, sorted by topic



COMPLAINTS

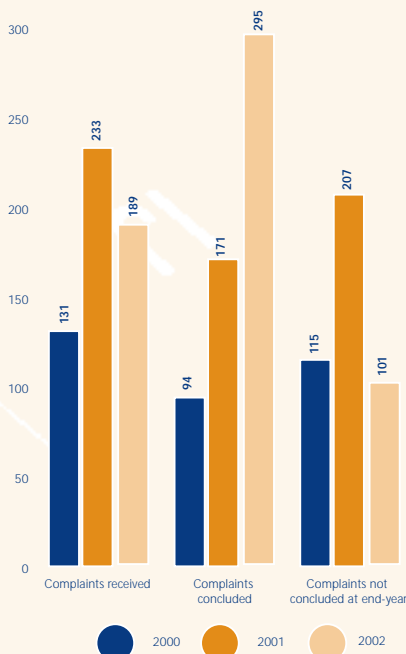
Individuals are entitled to complain to me if they consider that their Data Protection rights have been infringed in any way. Where a complaint is received, I, as Commissioner, am required by section 10 of the Data Protection Act, 1988, to investigate it, and, as soon as possible, issue a decision in relation to it. I regard this as the principal function of my Office. While complaints can often be resolved informally, to the mutual satisfaction of all sides, it is sometimes necessary for me to issue a formal decision on the matter. Such decisions are subject to a right of appeal by either party to the courts. (Under the 1988 Act, a complaint had to have been received or I had to be otherwise of opinion that there may be a

Part One - **Activities in 2002**

contravention of the Act before I could initiate an investigation. With the enactment of the Amendment Act I will have power to proactively carry out routine investigations as I consider appropriate to ensure compliance with the Act).

The additional staffing resources (see under Administration below) that have been allocated to my Office since late 2001 have had a marked positive effect on the processing of complaints. This is illustrated by the figures in Figure 4 below. Last year, I noted that while the figure for "complaints not concluded" had risen in both 2000 and 2001, I was confident that the allocation of much-needed staff resources would bring about significant improvements. I am glad to record that much progress was made in this regard last year as the figure for "complaints concluded" in the 12 months rose from 171 at end-2001 to 295 at end -2002 while the figure for "complaints not concluded" fell from 207 to 101 in the same period.

Figure 4 Complaints received, concluded and not concluded



During 2002, the number of new complaints processed formally was 189 compared with 223 the previous year. In real terms, the figures are 175 for 2001 and 182 for 2002 as the 2001 figure included 60 multiple complaints in respect of issues with 2 two separate Data Controllers while the 2002 figure included 9 multiple complaints in respect of 2 separate Data Controllers.

Figure 5 Breakdown of data controllers by business sector

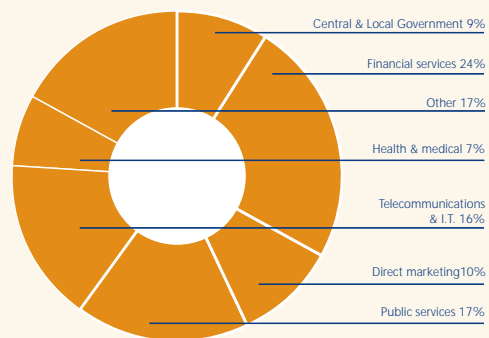
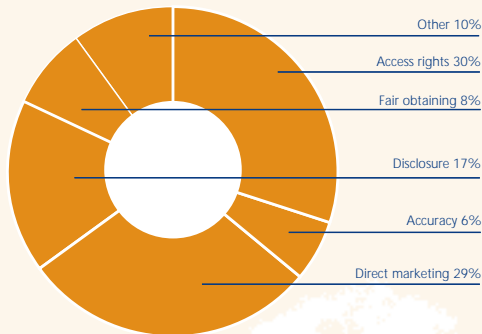


Figure 5 shows a breakdown of the types of organisation against which complaints were made to this Office in 2002. One-quarter of complaints concerned the financial services sector while telecommunications / IT and the direct marketing sectors accounted for a significant proportion of complaints. The public services and central and local government accounted for one quarter of complaints. As regards the grounds for complaint – see figure 6 – the largest single blocks of cases concerned the exercise of the right of access to data under section 4 of the Act (30%) and complaints about direct marketing (29%). Complaints about incompatible disclosures of data to third parties and about the issue of fairness were the next most common issue of complaint (together totalling 25%). The latter issues generally involve a lack of clarity or forthrightness on the part of a Data Controller in obtaining personal data, having regard to the uses to which the data will be put. Whether or not a disclosure is compatible can generally be answered by the simple test of whether the Data Subject would be surprised by the

Part One - **Activities in 2002**

disclosure. I would, therefore, emphasise what I have said in earlier Annual Reports; which is that unless a data controller is clear and up-front with a data subject, at the time when personal data are obtained, difficulties with data protection law are inevitable. Of the complaints concluded I found that 19% were upheld, 44% were resolved informally while 37% were rejected.

Figure 6 Breakdown of complaints by data protection issue



THE PUBLIC REGISTER

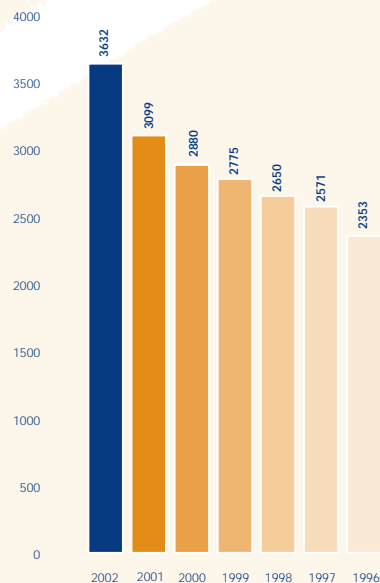
Under section 16 of the Data Protection Act, I am required to maintain a register of data controllers and data processors. The register is available for inspection by the public and is one of the ways in which transparency and openness in data processing can be achieved. The register gives an indication of the types of personal data being kept by organisations, and the purposes for which the data are used. The process of registration gives an organisation an opportunity to re-assess its data collection and retention policies, to ensure that – as required under the Data Protection Act – no excessive types of personal data are recorded, and that any data actually recorded are retained for no longer than necessary. Data controllers who are required to register in accordance with section 16 (generally, public bodies, financial institutions, bodies engaged in direct marketing, credit referencing and debt collection, telecommunications and internet access providers and holders of sensitive data as defined in the Act) are committing an offence if they process

data without being registered (section 19(6)). This is an area of Data Protection enforcement that I will be paying particular attention to in the current year as due to resource constraints up to now, I have had to rely to a great extent on ‘self registration’ by data controllers.

The number of persons registered had risen to 3,632 at the end of 2002, compared with 3,099 at the end of 2001 – an increase of 17%. Figure 7 shows the upward trend in the number of registrations over recent years. A more detailed sectoral breakdown of the registered persons is provided in Appendix 6.

During the year, my Office produced Registration Guidelines for the legal sector and the pharmacy sector. It is planned that Guidelines for other significant sectors will be produced in 2003 to help Data Controllers understand what is expected of them in the registration process. With the additional resources assigned to me, I will be seeking to ensure that registrations adequately describe the data processing operations covered and, as noted above, I will be taking steps to investigate the feasibility of providing on-line access.

Figure 7 Number of registrations



Part One - **Activities in 2002**

Registration of Telecommunications and Internet companies

In 2001, I promulgated the Data Protection (Registration) Regulations, 2001, which introduced a registration requirement for organisations providing Internet and telecommunications services to individuals. Internet and telecommunications services process considerable volumes of personal data in the traffic data that is generated when connections are made over networks. During the year, in the context of assessing applications for registration, I questioned the length of time that traffic data was routinely retained. This process brought to the fore the question of retention of such data for access, on an as required basis, by the Law Enforcement Authorities. The Minister for Justice Equality and Law Reform hosted a Consultation Forum on this matter in early 2003 to launch a public consultation on this important matter to inform the process of drafting legislation providing for retention of such data for Law Enforcement purposes (see Appendix 1). The process of accepting registrations from the Internet companies and telecommunications companies had been put on hold pending the clarification of retention policies. However, now that the Law Enforcement aspect is to be clarified in legislation, I am in a position to accept the applications on hand and these will now be finalised.

Registration and the Data Protection (Amendment) Act, 2003

The recently enacted Amendment Act provides for a change from the existing selective system of registration to a more comprehensive, 'universal' approach, as required by the terms of the European Data Protection Directive. The Act also provides that the Minister may issue Regulations exempting certain categories of organisation from the registration requirement. The Minister has undertaken to hold a Consultation Process on the registration requirements of the Act. For my part, I do not see the registration requirements as being an unnecessary burden on Data Controllers or Processors as I am only interested in registering those whose operations might have some significant bearing upon individuals' privacy rights. In this respect registration is an essential aspect of their Data Protection obligations.

Particular Sectors -Registration

Last year, I noted that the number of legal professionals registered with my Office was very small indeed. During the year, I engaged in correspondence with both the Bar Council and the Law Society and I am pleased to note that with their co-operation, the number of legal professionals registering with my Office on the basis that they process data of a sensitive nature relating to the health, criminal convictions or ethnic background of their clients, has increased. As of 1 April 2003, the number of Barristers on the Register was 80 while 51 Solicitors were registered.

This progress is positive and I will continue to keep the matter under review to ensure that the improvement noted continues. At the same time as examining compliance in the Legal profession, I am looking into the level of compliance in other sectors in order to ensure that the Register provides a comprehensive description of Data Processing operations of significance in the jurisdiction and is thus an effective tool in Data Protection compliance.

"Bogus" Registration Service

During the year, many companies received mailings from a UK company calling itself "Data Protection Act Registration Service" urging them to visit a bogus website, and to register under the Data Protection Act.

The bogus website, which was similar to our official website address, provided inaccurate and unreliable information regarding registration requirements under the Data Protection Act. They targeted companies who may not have been required to register but even if a company was required to be registered under the Act, availing of the "service" meant paying fees that were higher than the official fee. My Office immediately issued Press Releases highlighting the bogus nature of this service and referred the matter to the Garda Bureau of Fraud Investigation. The "Service" re-surfaced again in February 2003 and again the Office responded promptly by issuing Press Releases and notifying the Gardai who are currently investigating the matter.

Part One - **Activities in 2002**

LEGISLATIVE DEVELOPMENTS

Data Protection Directive

The Data Protection (Amendment) Bill 2002 was initiated in February 2002 to give effect to the EU Directive 95/46 on Data Protection. Following consideration by the Oireachtas the Data Protection (Amendment) Act 2003 was enacted in April 2003 and will become operational during 2003. However some of the Directive's provisions regarding security measures and transfers to non-EEA countries became effective from 1 April 2002 by regulations made by the Minister for Justice, Equality and Law Reform (Statutory Instrument No. 626/2001). The Regulations provide that

- *an organisation may not transfer personal data to non-EEA countries, which do not have an adequate standard of data protection, unless the organisation can point to other safeguards to protect peoples' privacy. Such safeguards could include appropriate contractual provisions, or the clear consent of the individuals in question. The EU Commission issues rulings regarding the adequacy of data protection levels in third countries, and regarding appropriate "model contracts" which organisations may use. Where the EU Commission has not made a ruling on such matters, the Data Protection Commissioner may be called upon to authorise a particular transfer of personal data, or to authorise particular types of transfer.*
- *the contractual rule regarding "privity of contract" is set aside in the case of "model contracts", or contracts approved for this purpose by the Data Protection Commissioner. This means that individuals are able to enforce contractual safeguards involving the handling of their own personal data by bodies outside the EEA, in the same way as if the individuals were themselves a party to the contract.*
- *data controllers must put in place appropriate security provisions for the protection of personal data, having regard to the current state of technological development, the cost of implementing security measures, the nature of the personal data, and the harm that might result*

from unauthorised processing or loss of the data concerned. In particular, the Regulations make it compulsory that the services of data processors - agents who process personal data on behalf of a data controller - should only be engaged on the basis of an appropriate written contract, together with other safeguards. The Regulations also clarified the territorial application of Irish data protection law to data controllers established in the State, and to data controllers established outside the EEA who process data in the State. Data controllers in the latter category must designate a representative in the State.

Telecommunications Directive

In 1997, the EU adopted Directive 97/66/EC in order to strengthen and clarify data protection and privacy rules in the telecommunications sector. This Directive has been implemented in Irish law by Regulations made by the Minister for Public Enterprise – the European Communities (Data Protection and Privacy in Telecommunications) Regulations, 2002 (Statutory Instrument No. 192/2002) – and came into effect on 8th May 2002. The Regulations set out the data protection standards that apply in the case of public telecommunications networks – including issues of security, privacy and direct marketing. The main provisions are

- *detailed records of people's telephone calls may be kept for as long as necessary to enable bills to be settled, but no longer.*
- *Telephone users have the right to block their phone number, so that it is not displayed to other telephone users.*
- *Individuals have the right to be excluded from public phone directories, or to have their address and gender omitted to protect their privacy.*
- *Individuals can sign up to a central "opt out" register, to indicate that they do not wish to receive unsolicited telephone calls. The register is under the overall superintendence of the Office of ComReg and will come into operation during 2003.*

Part One - **Activities in 2002**

- *Organisations who use automated calling machines which when activated operate to make marketing calls or faxes without human intervention must have the prior consent of individuals before these messages can be sent while companies can "opt out" from receiving them.*

A new EU Directive 2002/58 on Privacy and Electronic Communications was adopted in July 2002 to replace the existing Directive 97/66. It strengthens data protection rules across the whole telecommunications sector - including telephony, e-mails, internet use and SMS messaging - and will, for example, require companies to obtain positive "opt-in" consent before sending people unsolicited calls or e-mails. The Directive is due to be implemented in Irish law before 31 October 2003.

eCommerce Directive

In February 2003 the eCommerce Directive 2000/31 was transposed by Regulations made by the Minister for Enterprise, Trade and Employment (Statutory Instrument No. 68/2003). These require inter alia that an unsolicited commercial communication shall be clearly and unambiguously identifiable as such as soon as the recipient receives it.

Detailed notes on these legislative developments are available on my website <http://www.dataprivacy.ie/>

INTERNATIONAL ACTIVITIES

Data Protection cannot be confined to Ireland alone because with the ever-increasing globalisation of trade and the advance of the Internet any Commissioner cannot address privacy concerns in isolation. There is constant liaison at EU level but while other regions of the world may pose challenges in so far as adequacy of data protection is concerned, they can also provide new insights into how they approach data protection. That is why my Office participates in various international fora so as to ensure that universal privacy principles are applied. Much co-operation is achieved in the normal day-to-

day contact between fellow offices with attendances at international conferences kept to the minimum. The more co-operation and contact there is between my fellow Commissioners and offices ensures that peoples' rights can be respected world-wide as well as providing my office with valuable insights into developments in other regions of the world and in particular in developing countries. The range of international activities of my Office is accordingly outlined in the following paragraphs.

Article 29 Working Party

The Article 29 Working Party is a consultative body made up of the Data Protection Commissioners of the EU member states together with a representative of the EU Commission. The Working Party met regularly during 2002 and my Office participated in all of these meetings. The following were the main matters of interest discussed during the year:-

- *Concerns were expressed about the requests by the USA to have access to passenger manifest information and other data from airlines landing in the USA.*
- *The need to have a proportionate response regarding the mandatory systematic retention of telecommunication traffic data was emphasized.*
- *The harmonization of consumer credit laws in the EU needed to take account of privacy concerns.*
- *The matter of "Black Lists" raised sensitive and particular privacy issues.*
- *Certain on-line authentication services being offered by global IT companies raised particular concerns, which led to intense discussion with a major global computer concern.*
- *The international application of EU data protection laws to personal data processing on the Internet by non-EU based web sites was clarified.*

Part One - **Activities in 2002**

In addition the Working Party published an important working document on the surveillance of e-mail and Internet in the workplace as a follow up to its prior year document on the general aspects of processing personal data in the employment context. The document indicates that a workplace policy should be in place in an open and transparent manner and that

- *A balance is required between the legitimate rights of employers and the personal privacy rights of employees.*
- *Any monitoring activity should be transparent to workers.*
- *Employers should consider whether they would obtain the same results with traditional measures of supervision.*
- *Monitoring should be fair and proportionate with prevention being more important than detection.*
- *The document is a useful aid to employers, unions and workers and I propose to build on it in eventually drawing up a code of practice in this area. I intend to pursue this aspect in the coming year*

The detailed recommendations of the working party are available on the Commission's web site, which is accessible via the links section on my web site (<http://www.dataprivacy.ie/>).

EUROPEAN SUPERVISORY BODIES.

My Office continues to be involved in a number of bodies established to supervise the manner in which data are processed in certain European systems, including Europol, Schengen, the Customs Information System and Eurodac. These supervisory bodies meet in Brussels a number of times each year.

Supervision of Europol.

Apart from the routine work conducted by the Joint Supervisory Body, the initiative taken by the Danish Presidency of the Council of Ministers to amend the Europol Convention has been the subject of discussion at the JSB.

National Supervision of Europol.

Alongside my role on the JSB Europol, I am also the National Supervisory Authority of Europol. In that context, my staff have visited both the Europol National Unit of An Garda Síochána in Dublin and the Garda Liaison office in Europol Headquarters located in the Hague, the Netherlands. It is my intention to conduct a formal inspection of these offices during the course of 2003.

Europol JSB Appeals Committee.

There were a number of meetings of the Appeals Committee of the JSB to consider appeals from data subjects concerning the processing of their data by Europol. The Committee issued its first decision on an appeal during the course of 2002.

Schengen Joint Supervisory Authority.

The Schengen Convention of 1990 allows for the free movement of persons between participating States. Ireland has applied for partial membership and until such time as measures have been taken to implement Schengen, my Office attends meetings of the JSA in an observer role.

Schengen evaluation.

During the Danish presidency of the Council of Ministers, an evaluation of the operation of Schengen in the Benelux countries (Belgium, the Netherlands & Luxembourg) was undertaken. My staff participated in the data protection elements of the evaluation, which proved to be a valuable experience, assisting preparations for our implementation of Schengen

The Customs Information System Joint Supervisory Authority.

Whilst a number of meetings took place during the course of 2002, the information system has yet to go live.

Part One - **Activities in 2002**

Eurodac.

Eurodac is a system facilitating the exchange of fingerprint data relating to asylum applicants. This system went live in early 2003, while the first meeting of the Joint Supervisory Body took place in November 2002, which I attended. This meeting agreed the rules of procedure for the supervisory body, which will cease to exist following the appointment of the EU Data Protection Supervisor- a new post, created to supervise data protection in the EU institutions.

INTERNATIONAL CONFERENCES AND WORKING GROUPS

Annual International Conference of Privacy and Data Protection Commissioners

The 24th annual International Conference of Privacy and Data Protection Commissioners was held in Cardiff in September 2002. In line with the spirit of co-operation that exists between the islands, the conference was successfully co-hosted by the data protection commissioners of Ireland, the United Kingdom, Jersey, Isle of Man and Guernsey. This was the first occasion that Commissioners combined to host this major conference, which was attended by over three hundred delegates. The United Kingdom Commissioner and a Cardiff "events" organising company are complimented for a very successful operation as they undertook most of the organising arrangements.

The Conference allows data protection authorities from around the world and other interested parties, from both the public and private sectors, to come together to discuss developments of common interest. The Conference debated and evaluated key challenges within data protection and freedom of information. Topics addressed covered a broad range of business and consumer issues including information sharing, identity cards, self-regulation, the role of technology, freedom of information, the role and image of the data protection authorities. In particular it discussed whether the following propositions were myths or realities

- *Data protection principles, by preventing information sharing, hold back both modern government and efficient business*
- *Anonymity has no place in the age of global information systems and international terrorism*
- *Effective data protection can only be delivered through independent powerful supervisory authorities.*

My deputy commissioner and I chaired two of the three public plenary sessions while Kevin Murphy, the Information Commissioner and Ombudsman and Oliver Ryan, the Director of the Reach Agency made significant presentations to the Conference. I am grateful for their participation as they outlined in detail how Ireland is addressing the challenges that are arising in this whole area of data access, sharing and eGovernment in a data protection compliant manner.

During a session of the Conference confined to Commissioners, privacy issues in relation to web sites and surveillance in public and private places were discussed. However the Commissioners devoted a substantial amount of time to considering the various national responses to the terrorist attacks of September 11th, 2001. The Commissioners agreed that whilst there is the need to protect society from these outrages the reactions in many countries might have gone beyond a measured response to the terrorist threat with serious implications for personal privacy. The need to safeguard personal privacy in such developments remains an essential task for the worldwide data protection community. Unless Governments take an approach that correctly weighs data protection and privacy concerns there is a real danger that they will start to undermine the very fundamental freedoms they are seeking to protect.

Finally I am honoured that the Australian Commissioner, who is hosting the 2003 Conference, asked me to participate on a working group, of international public and private people, to assist him in devising the agenda for the Conference. All our deliberations have been conducted via the Internet.

Part One - **Activities in 2002**

Spring Conference of European Data Protection Commissioners

This long-established annual international forum took place in Bonn in April 2002. The Spring Conference is attended by Data Protection Commissioners from the whole of Europe, not just those in the EU. The deputy commissioner and myself participated in the Conference, which discussed security legislation, privacy audits, biometrics, eGovernment and closer co-operation with Eastern European data protection commissioners.

A further meeting of the Conference was held in September 2002 in conjunction with the International Conference. This meeting noted with concern that in the third pillar of the EU, proposals were being considered which would result in the mandatory systematic retention of traffic data concerning all kinds of telecommunication (i.e. details about time, place and numbers used for phone, fax, e-mail and other use of the Internet) for a period of one year or more, in order to permit possible access by law enforcement and security bodies. Grave doubts were expressed as to the legitimacy and legality of such broad measures. The Commissioners stated that systematic retention of all kinds of traffic data for a period of one year or more would be clearly disproportionate and therefore unacceptable in any case. Attention was drawn to the excessive costs that would be involved for the telecommunications and Internet industry, as well as to the absence of such measures in the United States. It concluded that where traffic data are to be retained in specific cases for security purposes, there must therefore be a demonstrable need, the period of retention must be as short as possible and the practice must be clearly regulated by law, in a way that provides sufficient safeguards against unlawful access and any other abuse. This position was formally endorsed later in October 2002 by the Article 29 working party.

International Complaints Handling Workshops

These twice-yearly international complaints handling workshops to discuss approaches to complaints handling procedures have proven informative and effective. Personnel who deal with complaints from the European data protection offices meet to discuss case management and emerging trends. They also compare the different approaches in use across Europe for investigating breaches of data protection legislation with the aim of achieving reasonable harmonisation.

My Office had the honour to host the Fifth Complaints Handling Workshop in Dublin in March 2002. I congratulate my Office staff for the organisation that went into making it an effective and productive event. Thirty delegates attended the two-day meeting including the newly appointed Hungarian Data Protection Commissioner. A variety of topics were discussed, including different levels of access to health data; problems arising from transborder data flow; entry rules for the web-based forum established to facilitate and build upon the workshop; the proposed "solvit" network of the EU Commission; a proposal for a privacy survey on on-line banking and the various approaches adopted by offices in relation to a complaint about direct marketing. The need for a common policy across the EU in respect of transborder data flow, especially relating to the transfer of human resources data to other elements of multinational companies, was also considered. Having experienced the operation of the workshop at first hand I appreciate its usefulness. Though still in its infancy I can see its potential, not just in dealing with complaints handling, but also as a means of exchanging information on a broad range of data protection issues at a practical and functional level.

The sixth workshop was held in Berlin in November 2002 where two of my staff attended a very productive meeting.

Part One - **Activities in 2002**

International Working group on Data Protection in Telecommunications

A long established working group comprising data protection commissioners from various countries meets twice yearly to consider privacy and data protection in the communications and media areas. The Berlin data protection commissioner provides the secretariat for the group. Due to resource constraints Ireland had not participated in the group in the recent past but it was possible to redress that situation during 2002. I attended the meeting in Auckland, New Zealand in March 2002 while my deputy commissioner attended the Berlin meeting in November 2002. We have found this working group particularly useful and we intend to participate in many of its future meetings. Topics considered included telemedicine sites, children's on line Internet policy, public data bases, identification on online systems, retention of traffic data, Cybercrime Convention, Spam and media privilege.

Asia Pacific Forum on Privacy and Data Protection

In conjunction with the Auckland telecommunications meeting the Privacy Commissioner of New Zealand organised a forum on freedom of information and data protection. I outlined Ireland's data protection laws and how my Office operated. As the forum was also discussing responses to the September 11th attacks and their possible impact on privacy I gave details of developments in Europe and in Ireland. Commissioners from Canada, Australia, Hong Kong, Japan and Singapore attended as well as representatives from many other privacy offices.

British and Irish Data Protection Authorities Meetings

Finally, the British and Irish data protection authorities (including those from the Isle of Man, Guernsey and Jersey) met in Dublin during May 2002 to exchange information and views on matters of common concern. The meeting focused in the main on planning for the Cardiff International Conference.

ADMINISTRATION

Running Costs

The costs of running the Office in 2002 are as set out in Table 1 below. Figures for 2001 are given for comparison.

Table 1 Costs of running the office in 2002

	2001 (€)	2002 (€)	% change
Overall running costs	588,709	815,173	43%
Receipts	341,758	350,666	3%

The increase in running costs was mainly due to the increase during the year in the staffing of the Office from 8 to 16. A fuller account of receipts and expenditure in 2002 is provided in Appendix 5.

Part One - **Activities in 2002**

Staffing

The steady growth in the number of staff during the year to 16 has meant that the Office is now reasonably well placed to respond to the challenges which will be posed in implementing the Data Protection (Amendment) Act, 2003. The full authorised complement for the Office is 21 and the filling of all of these posts is vital if the Office is to be able to adequately discharge the additional workload which the new Act will, undoubtedly, bring in terms of the increasing – and increasingly complex – requirements of data protection law and its enforcement. The new Act will also mean that we will have to change the way we do our work, as I now have new powers to pro-actively carry out investigations and privacy audits where I consider this necessary. I wish to acknowledge the continuing positive response of the Department of Justice, Equality and Law Reform and their understanding of our needs in this regard.

Support Services

The technological environment within the Office was reviewed during the year by the IT Section of the Department of Justice, Equality and Law Reform and has been upgraded where necessary. I wish to record my appreciation of the work of the Department's IT personnel. I am also happy to record my appreciation of the Department's Finance Division, based in Killarney, which has continued to provide my Office with a vital service in the area of receipts and payments.



Part Two

Case Studies

Part Two Case Studies

Case Study 1

Motor Insurance - excessive information-marital status not necessary

I received a complaint about a practice among motor insurance companies of asking applicants an excessive number of questions. The complainant considered that some questions had no relevance, in particular the one relating to marital status. He was of the opinion that the information sought had more to do with customer profiling than assessing insurance risk.

The insurance companies informed me that marital status is not taken into account in a decision about insurance. However they considered that they needed this information because if an issue about alleged discrimination arose in the future in regard to marital status, it would have to be able to have supporting evidence to comply with the Equal Status Act. I found this reasoning difficult to accept.

Under section 2 of the Act, data sought should be adequate, relevant and not excessive in relation to the purpose for which it is obtained and held. **I considered that details of a person's marital status is irrelevant to the question of motor insurance and requested that this question be deleted from questions asked of prospective customers. Of course, if a person wishes to include a named driver on the policy, it is reasonable and relevant that the relationship be indicated.**

I am pleased to record that the companies agreed to delete the question and I trust that all companies in the industry are so doing.

details of a person's marital status is irrelevant to the question of motor insurance

she heard 'pips' on the line and, on enquiring, was informed that the call was being recorded but no explanation for the recording was given by the person representing the bank.

Case Study 2

International Bank-recording of telephone calls-lack of transparency-legitimate business interest-satisfactory response

I received a complaint from an individual who stated that in the course of her employment for a particular company she received a telephone call from one of the major international banking organisations based in Ireland. In the course of the call, she heard 'pips' on the line and, on enquiring, was informed that the call was being recorded but no explanation for the recording was given by the person representing the bank.

My Office contacted the banking organisation involved and inquired why people were not made aware that such recording was taking place and the security procedures in place. It clearly is important in Data Protection terms that an individual is aware of and gives consent to such recordings. I, of course, appreciate that in the financial world it can be necessary when telephone instructions are given that some record has to be available in case a dispute arises.

In response the bank stated that, in line with industry practice in the financial services sector in Ireland, it operated an automated telephone recording system. Under this system, calls are automatically recorded and the recordings are retained for one year. Access to these recordings, permitted only under strictly controlled conditions, is limited either to where evidence is required in the case of a dispute by a customer as to an instruction or confirmation given, or where there is an investigation of suspected fraud or other criminal activity. Only a limited number of senior individuals had access to the recordings, which are kept in a secure room in a secure locked cabinet and then only where documentation had been completed and approved.

Part Two - Case Studies

The bank initially disputed whether personal data was involved, arguing that although the system was capable of automatic operation in that it listed details of particular calls made at a particular time, to or

from a particular telephone number, it was questionable whether the recordings contain data relating to an 'identifiable individual'. **It was explained to the bank that, from a data protection perspective, it had the capacity to identify the individual by accessing the telephone recording system and using this in conjunction with other data held by the company thereby bringing it within the scope of the Data Protection Act.**

The bank also indicated that their target market in Ireland is aimed at a strict market consisting of multinational corporates, financial institutions and the Government and that their business in Ireland was not retail based. It stated that the telephone recording system which they operated at the time of the Office's enquiry was first implemented in 2000 and did not have the capability of restricting the recording of calls to specific telephone extensions or business critical areas. It was in the process of installing a new system which would have the capability to limit the recording of calls to business critical areas only. It was also introducing automated messages within the telephone system which would advise that the call was being recorded and the purpose of the recording. **I consider that a legitimate interest basis exists for the recording of calls in business critical areas in the financial services sector, subject to the proviso that callers should be clearly informed that recording is taking place and the caller can then either go on with the call or not.**

Clearly in this case there was not sufficient transparency in relation to the recording of calls - 'pips' on the line would not normally alert somebody to the fact that the call is being recorded. However, I am satisfied that the bank have now addressed this satisfactorily by the automated messaging system, limiting the recording of calls to business critical areas, advising callers that phone calls are being recorded and the purpose of the recording.

I am glad that this important matter which has wider application was brought to my attention and I also appreciated the time taken and the manner in which this banking organisation addressed the issues raised in a constructive manner.

Case Study 3

Gardai- Inappropriate data on “Pulse system” -data deleted when access request received- not fair to person- could frustrate the provisions of the Act

A person contacted my Office as she believed that An Garda Síochána were holding data about her on their “PULSE” database which was untrue. The complainant had made an access request to An Garda Síochána under section 4 of the Act but she did not believe that this request had been complied with, as she believed certain details had not been furnished to her.

I raised the matter with An Garda Síochána, which cooperated fully with my enquiry. I asked them to confirm if an entry had been made on the PULSE system about the complainant and if so,

- *had it existed on the date on which the access request was made?*
- *why had it not been released to the complainant in response to the access request?*
- *did the entry still exist?*
- *if the entry no longer existed, when had it been deleted and what had been the circumstances of the deletion?*

An Garda Síochána responded that following receipt of the access request from the data subject, a search was carried out of the databases on PULSE for relevant personal data. In addition to the data supplied in their response to the access request, they said that the search also revealed a comment relating to the data subject. On examination of the comment, An Garda Síochána stated that a decision was taken by them that the comment was inappropriate and it was therefore deleted.

I noted this response and I informed An Garda Síochána that I could well understand - indeed accept - why they decided to delete the information, which they considered to be inappropriate. However, I pointed out that once an access request is made,

the search also revealed a comment relating to the data subject. On examination of the comment, An Garda Síochána stated that a decision was taken by them that the comment was inappropriate and it was therefore deleted.

then any personal data on the system on the date of receipt of the request has to be supplied in line with section 4(1) of the Act. Under section 4(5), it is not permissible to delete or edit data following receipt of an access request - only up dating of data which would have taken place in the normal course is permissible.

In the circumstances, I found that An Garda Síochána should have supplied the data in question to the data subject but they should have outlined that, on examining it, they had decided to delete it as they considered it to be inappropriate and not in line with the provisions of section 2 of the Act which requires data to be accurate and up to date. In essence, what this means is that once a subject access request is received, the subject access request power under section 4 is not to be frustrated by using the power under section 2 for the deletion of inaccurate data. **Information should only be recorded if it is of operational significance, on the basis of a judgement that the information is likely to be of assistance to An Garda Síochána in the exercise of its lawful functions. Recording of data on a system should be accurate and informed but not inappropriate. Any information that does not reach this standard must be considered irrelevant and/or excessive, and should form no part of Garda records.**

I recognise that in the Garda area recording of information and opinion is vital for the prevention, detection and investigation of crime and that they may have concerns that access requests could frustrate their work. However, section 5 of the Act provides for restrictions on the right of access to personal data in certain cases (for example, where access could prejudice the prevention, detection or investigation of crime) and this provides adequate cover to ensure that their work is not hindered.

Accordingly, I requested that they revise their procedures to ensure that section 4 requests are fully complied with and that a similar type situation cannot arise in future. This I am glad to report has been acted on and it seems to have been an isolated though highly important case.

political canvassing messages came within the terms of the Regulations and as such were a form of direct marketing

Case Study 4

Data protection in the telecommunications area- automated telephone marketing - political canvassing- text messages to mobile phones-national opt out register

EU Directive 97/66 stipulates the data protection standards that must apply in the case of public telecommunications networks including issues of security, privacy and direct marketing. It was transposed by Regulations into Irish law with effect from 8th May 2002. The Regulations include the following measures to respect the rights of people who do not wish to receive unsolicited telephone calls for direct marketing purposes

- *a single, national register on which people can indicate that they do not wish to receive unsolicited telephone calls to be supervised by ComReg. Direct marketers must consult this national 'opt out' register, and the wishes of subscribers must be respected. Individuals who wish to be included in the 'opt-out' register – i.e. individuals who do not wish to receive unsolicited telephone calls – should notify their telecommunications company, which will make the appropriate arrangements. Subscribers with unlisted numbers will automatically be included on the 'opt-out' register.*
- *the use of automatic dialing machines (i.e. when activated operate to make calls, including sms text messages, without human intervention) to call individual subscribers at random for direct marketing purposes, being prohibited, unless subscribers' consent has been obtained in advance. Unsolicited fax messages to individual subscribers are likewise prohibited.*
- *companies, societies and other organisations are afforded some data protection rights, for the first time. Such organisations may 'opt-out' of receiving unsolicited telephone calls – including randomly dialed calls and unsolicited faxes – by signing up to the national 'opt-out' register.*

During 2002 I received complaints from various sources on the use of automatic dialing machines for marketing calls. One concerned the issuing of sms text messages to mobile phones by a phone marketing company. A second concerned a company which complained that it was receiving many unsolicited fax messages from various sources. Another arose when several people complained about canvassing by a political party and by a candidate prior to the 2002 General Election where automated dialing machines were used to deliver recorded messages.

I investigated these complaints and

- *the phone company immediately ceased issuing the sms text messages once I made urgent phone contact with it following receipt of the complaint. The requirements of the regulation were discussed later in detail with it and guidance was issued as to what "human intervention" meant.*
- *in the absence of the national "opt out" register being in operation, I could have been unable to address the matter. However, I did contact the fax issuing company who removed the company's name from its database. The "opt out" register should, however, be up and running during 2003.*

Regarding the complaints about political canvassing the question arose as to whether it was a form of direct marketing in data protection terms. Though the Data Protection Act, 1988 or the Regulations do not define direct marketing in detail it can cover a wide range of activities as

- *the Council of Europe stated in 1985 that direct marketing comprises all activities which make it possible to offer goods or services or to transmit other messages to a segment of the population by post, telephone or other direct means aimed at informing or soliciting a response from the data subject as well as any service ancillary thereto.*

Part Two - Case Studies

- *the Federation of European Direct Marketing (FEDMA) which represents Direct Marketing bodies in Europe indicated in 1998 that “direct marketing is a series of marketing strategies, using various delivery techniques designed to provide the receiver (consumers and companies) with information at a distance by using different means of approach e.g. broadcasting, printed press, mail, telephone, on-line-service. It is used to sell products, to deliver information, to make public announcements, for sales after-service, for customer care services, charity and political appeals”.*
- *the United Kingdom Information Commissioner has expressed the view that direct marketing will apply not just to the offer of goods or services, but also the promotion of an organisation’s aims and ideals. This would include a charity or a political party making an appeal for funds or support and, for example, an organisation whose campaign is designed to encourage individuals to write to their MP on a particular matter or to attend a public meeting or rally.*
- *I recognise and accept that the need for candidates in an election to contact as many potential voters as possible is fundamental to the proper operation of the democratic process. I am, however, of the opinion that to protect the privacy of telephone subscribers a broad view should be taken particularly in the area of telecommunications contacts made without human intervention using automated equipment.*

I therefore considered that the political canvassing messages came within the terms of the Regulations and as such were a form of direct marketing. I accepted that they were made in good faith but I upheld the complaints. It was appropriate for me to note in reaching my decision that the Regulations only came into force on 8th May 2002 and that the messages were transmitted on 16th May 2002. This short period placed the contravention in context and both have assured me, and I accept, that it was not their intentions to breach the regulations.

I should add that since I made my decision the Data Protection (Amendment) Act 2003 has defined direct

marketing as including “direct mailing other than direct mailing carried out in the course of political activities by a political party or its members, or a body established by or under statute or a candidate for election to, or a holder of, elective political office”. This brings necessary clarity to this area.

These complaints bear out the public awareness survey findings, outlined in Appendix 2, that direct marketing, regardless of the medium used, is more likely to earn the thumbs down than the approval of people with, predictably, resistance being the strongest to direct marketing attempts via the home telephone.

Case Study 5

Telephone Company -alleged disclosure of customer call related information at the request of the Gardai - Information Notice issued.

A journalist complained to me that she had requested from her telephone service provider a list of all the individuals who had made enquiries in relation to her mobile telephone account and that in response she had been given a printout of all the requests and enquiries which she herself had made. On further enquiry, she was told that the company had no record of any third party requesting information on [her] account. The complainant told me that she had evidence that Gardai had accessed confidential billing information from her account but that the company were stating that they had no record of anyone other than her requesting such information.

I investigated the matter fully and due to its nature, detailed and complex issues arose.

In regard to the right of access to one's data as provided by section 4 of the Act, I noted that this can be restricted in certain circumstances by section 5 in respect of personal data

(a) kept 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 that section to the data would be likely to prejudice any of the matters aforesaid,;

In regard to the alleged disclosure to the Gardai, the Act does not impose a blanket prohibition upon the disclosure of personal data because section 8 of the Act specifies a number of restricted circumstances in which the clear statutory bar on the making of such disclosures is lifted. Such circumstances include safeguarding the security of the State (section 8(a)), a requirement for the purpose of preventing, detecting or investigating offences or prosecuting offenders, in cases where the application of the nondisclosure rule would prejudice such matters (section 8(b)), or a requirement by or under any enactment or rule of law or order of a court (section 8(e)).

the Gardai and telecommunications companies are aware that I have an oversight power and is an assurance to them and the general public that in this sensitive area such an oversight power can be exercised when necessary.

I noted that the Postal and Telecommunications Act, 1983, as amended by the Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993, makes provision for the disclosure of customer call related information by telecommunications operators at the request of An Garda Síochána or the Defence Forces. The Act also sets out the procedure that must be followed in such requests e.g. the request must be signed by a member of An Garda Síochána not below the rank of Chief Superintendent or not below the rank of Colonel in the Defence Forces. Such disclosures would be covered under section 8(e) of the Data Protection Act. The Postal and Telecommunications Act, 1983 also provides that a telecommunication provider is prohibited from disclosing information relating to requests for information made by An Garda Síochána, or indeed confirming whether such requests have been made by An Garda Síochána.

The matter was taken up by my Office with the company who referred to the Telecommunications legislation quoted above and to the restrictions provided in it as to the circumstances in which it could not confirm or deny to my Office whether or not any request for customer call related information had been made by or provided to the Gardai in this case. I considered the response to be unsatisfactory but understandable to a degree. Accordingly I considered whether, in the light of my powers under section 12 of the Act, to issue an information notice requiring the furnishing of specified information. Section 12(4) provides that where the Commissioner issues an information notice

(a) No enactment or rule of law prohibiting or restricting the disclosure of information shall preclude a person from furnishing to the Commissioner any information that is necessary or expedient for the performance by the Commissioner of his functions.

(b) Paragraph (a) of this subsection does not apply to information that in the opinion of the Minister or the Minister for Defence is, or at any time was, kept for the purpose of safeguarding the security of the State or information that is privileged from disclosure in proceedings in any court.

Because of the nature of this complaint I decided that such an information notice be issued so that I could fully investigate the complaint. The information notice was complied with by the company and was responded to within the 28 day time limit.

Following further consideration of the response, I found that the company had not contravened any of the provisions of the Data Protection Act in this instance. In so deciding **I did not confirm or deny that the Gardai had sought or received the information in question as to do so could frustrate the powers of inquiry of the Gardai in their normal work. However my actions ensured that the Gardai and telecommunications companies are aware that I have an oversight power in this area and is an assurance to them and the general public that in this sensitive area such an oversight power can be exercised when necessary.**

Case Study 6

Women's Mini- Marathon-unauthorised and incompatible disclosure-Internet photographs-informed consent.

I received a complaint from a mother who took part in the Women's Mini-Marathon in June 2002 with her fourteen year old daughter. Her daughter subsequently received a letter in July 2002 from a UK company offering her photos of herself taken on the day of the marathon. The photos also appeared on the company's website. The mother complained that she had not given permission to the organisers of the mini-marathon to supply her daughter's name, address and race number to another company or to take photos of her daughter and she had requested that the photo be removed from the website immediately. The photos were subsequently removed from the web-site at the request of my Office. **The Data Protection issue here involved the disclosure of personal data in a manner incompatible with the purpose for which it had originally been obtained.**

My Office contacted the organisers of the mini-marathon who agreed that they had supplied the information to the company to take photos on the day and that the participants would not have been aware of this when they signed up for the event. The organisers hoped if this proved popular that they would engage the company to take photos the next year. The organisers made facilities available to the company to take photos at the start and finish of the race. They gave them access to their database of participants and the company offered photos to these participants for sale.

the entry form did not indicate the further use to which the database of entrants would be put and it should have provided for prior consent to be given or withheld.

Part Two - Case Studies

While acknowledging the view of the race organisers that this service was of added value to participants and was part of the race experience, I considered that a contravention of Data Protection Law had occurred in this instance in that the entry form did not indicate the further use to which the database of entrants would be put and it should have provided for prior consent to be given or withheld.

My Office arranged a meeting with the organisers of the event at which the data protection requirements for events of this nature were discussed in detail and in particular, the obligation regarding transparency as to the uses to which information would be put. This involved a minimum requirement that a facility to opt out of additional uses be provided. The organisers agreed to revise their procedures for future events, and to give participants an option regarding photos.

I was satisfied with the response of the organisers of the Women's Mini Marathon to the complaint, and I note that they revised their entry forms to reflect Data Protection requirements for the forthcoming 2003 event.

companies cannot assume that it is in their customers' interests to pass on their details to others - they can only do so, with the customer's consent.

Case Study 7

Spanish apartment purchase- disclosure of Data to Third Party without consent- well meaning intention not good enough

I received a complaint from an individual who had purchased a property in Spain. The individual had subsequently received two letters to his home address advertising a furnishing service. The complainant discovered that the furnishing company had obtained his details from the property agent.

The matter was investigated by my Office and the property agent stated that his employee had passed on the details, on her own authority, in good faith, as many clients had sought information on companies that could provide a furnishing service in Spain. On receiving the complaint, he contacted the furnishing company immediately and requested them to remove the individual's details from their mailing list. No other disclosure of data to third parties had occurred.

Section 2(1)(c)(ii) of the Data Protection Act, 1988 provides that personal data "shall not be used or disclosed in any manner incompatible with" the purpose or purposes for which it is kept. I was pleased to note that the property agent had taken immediate and appropriate steps to address the issues involved in this case, particularly in terms of ensuring that appropriate security measures were in place and in improving awareness of staff and management regarding the importance of not disclosing data for an incompatible purpose to third parties.

This case illustrates that companies cannot assume that it is in their customers' interests to pass on their details to others - they can only do so, with the customer's consent.

Case Study 8

Department of Defence-deafness compensation data supplied to another Department- unauthorised disclosure-good intentions but anti-fraud measures must respect prejudice test of data protection law-Government is not a single data controller

I received a complaint from a serving member of the Defence Forces who had obtained damages arising out of a civil action taken by him against the Minister for Defence regarding a deafness complaint. He alleged that details of this settlement had been forwarded by the Department of Defence to the Department of Social and Family Affairs for the purposes of checking if he was in receipt of Social Welfare means tested payments.

On inquiry with the Department of Defence I established that the Department of Social and Family Affairs had sought details from the Department of Defence in November 1999 of compensation claims for hearing loss, which were being paid to ex-members of the Defence Forces. The Department said in its request that "it is possible that some of the many compensation claims currently being paid to ex-members of the Defence forces should be assessed as means for Social Welfare payments. I am anxious to test the possibilities". The Department of Defence had provided in January 2000 a list of all claims for hearing loss where an Award or Settlement had been made. This list contained details of 4,275 claimants. I noted that the Department did not establish if the details being supplied were in respect of ex-members of the Defence forces who were in receipt of Social Welfare payments.

I am as concerned as anyone that appropriate antifraud measures are taken by any organisation and in particular where State moneys are involved. I can well appreciate why the Department of Social and Family Affairs would explore any avenue of possibility. Nevertheless this case raised important and complex issues relating to the conditions which need to be met for personal data to be shared between Government Departments.

each Government Department is a Data Controller in its own right - Government is not a universal Data Controller- and there are mechanisms in place in Social Welfare and other Laws for the exchange of personal data, as necessary

Questions arose as to whether the Department's purpose in processing claims could be said to include the protection of public funds by another organ of the State, whether the disclosure to the Department of Social and Family Affairs could be considered to be a compatible purpose and whether a "public interest" test could be used as a basis for the disclosure.

These matters were raised by my Office with the Department of Defence who justified the disclosure on the basis that

- *The initiation and maintenance of legal proceedings in this case, as with others, was a matter of public record.*
- *The settlement by the State of the claim, out of public funds, was not the subject of any agreement on confidentiality between the parties.*
- *The provision of information on the fact and amount of the settlement by one Department of State to another to ensure the proper administration of the Social Welfare Code was entirely proper and appropriate.*
- *Section 8(b) of the Data Protection Act, 1988 provides that restrictions 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, duties or other monies owed or payable to the State....".*

Part Two - Case Studies

Section 2 of the Data Protection Act 1988 provides that data “shall be kept only for one or more specified and lawful purposes and shall not be used or disclosed in any manner incompatible with that purpose or those purposes”. It was clear to me that the data in question was generated for the purposes of processing applications for compensation and for managing the civil actions and associated settlements, which arose. I questioned whether this included assisting other agencies of the State charged with investigating offences against the State (including the tax and social welfare codes).

The Department accepted that there was no explicit statutory provision for the disclosure. It maintained, however, that the protection of public funds from the possibility of a second claim was encompassed within the purpose. While the Department, of course, has an obligation to ensure that it spends public funds appropriately and for the purposes for which they are voted by the Oireachtas, it has no direct responsibility or accountability for the expenditure of another Department. Indeed, I found it difficult to understand how, in the absence of clear evidence that public funds had been abused, that the data was released. In the absence of a statutory provision at the time, or clear evidence that public funds had been abused in specific cases, the Department of Defence could not assume a new purpose for the data retrospectively as a basis for disclosure. Furthermore the Department did not establish if the details supplied were in respect of ex-members of the Defence forces who were in receipt of Social Welfare payments.

The data protection rule that disclosures of information must always be compatible with the purposes for which that information is kept is lifted in certain cases by section 8 of the Act. Section 8(b) provides that restrictions 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, duties or other monies owed or payable to the State in any case in which the application of those restrictions would be likely to prejudice any of the matters aforesaid.”

While the request from the Department of Social and Family Affairs for details of recipients of compensation was stated to be for the purpose of preventing, detecting or investigating such offences, the Department of Defence failed to take account of the significance of the words “in any case”. The effect of the provision in 8(b) is that a disclosure is permitted - and the Department has discretion about whether to give the data - only in cases where non - disclosure would be likely to prejudice the prevention, detection or investigation of offences. This is a prejudice test whereby it must be clearly established in specific cases that non - disclosure of particular personal data would prejudice any of those matters.

I then considered the question of the “public interest” and “the protection of public funds” as a basis for the disclosure in detail. Section 222 of the Social Welfare (Consolidation) Act, 1993 provides that

“Information held by the Minister for the purposes of this Act or the control of schemes administered by or on behalf of the Minister or the Department of Social Welfare may be transferred by the Minister to another Minister of the Government or a specified body and information held by another Minister of the Government or a specified body which is required for the said purposes or the control of any such schemes administered by another Minister of the Government or a specified body may be transferred by that Minister of the Government or a specified body to the Minister”.

I consider that this is a general facilitating provision for the exchange of data between the Department of Social and Family Affairs and other Departments for the specific purposes of the control of Social Welfare schemes in specific cases where there would be a substantial risk that public funds could be abused, rather than a mere chance. It had to be read with section 8(b) of the 1988 Act, such that a disclosure is permitted only where non - disclosure would be likely to prejudice the prevention, detection or investigation of offences in any case. I did not accept that the exchange of a whole set of data for the purposes of data matching, as what happened in this case, met these conditions. In this specific case - and possibly others - the complainant was a serving member of the Defence Forces and it was not established if he or

Part Two - Case Studies

his dependants had applied for and /or were in receipt of or entitled to Social Welfare entitlements.

I take the view that if it were in fact the case that personal data could, and indeed should, be shared among Government bodies other than in specific cases, there would have been no need for the Oireachtas to introduce the detailed and complex provisions of the Social Welfare Act, 1998, Part IV (sections 14 and 15), which were inserted into section 223 of the Social Welfare Consolidation Act, 1993. In particular, section 223C provides:

"(2) A specified body holding information may share that information with another specified body who has a transaction with a natural person relating to a relevant purpose, where the specified body seeking the information provides the personal public service number of the person who is the subject of the transaction and satisfies the data controller of the specified body holding the information that the information requested is relevant to the transaction for the said purpose between the person and the specified body seeking such information".

These provisions were introduced in order to provide a framework for the exchange of personal data among "specified bodies" (including Government Departments, local authorities and certain other public bodies) in certain tightly-defined circumstances, and to allow the Personal Public Service Number to be used as a common identifier for this purpose. Neither would there have been a need for the Health (Provision of Information) Act, 1997 (which allows personal data to be shared within the health sector for cancer screening purposes) or the Housing (Miscellaneous Provisions) Act, 1997 (section 15) which was introduced in order to allow An Garda Síochána and certain other bodies to share personal data with housing authorities, thereby overriding the bar upon such disclosure contained in the Data Protection Act.

In the circumstances, I found that the Department contravened the "purpose" and "compatible disclosure" principles of section 2 of the Act.

While I upheld the complaint, I noted that the Department undertook that in future personal data of the type in question will only be provided to the Department of Social and Family Affairs in accordance with the procedure provided for in section 223C of the 1993 Act i.e. on request from the Department of Social and Family Affairs in specific cases. I also noted that this would not cause any difficulties regarding data protection law as Section 8(e) of the Data Protection Act, 1988 allows for "disclosures which are required by an enactment" .

The Department did not appeal my decision to the Circuit Court. As the matter was of a complex nature the decision was only arrived at after careful consideration of all the arguments put forward by the Department. I accept that the Department acted in good faith in this case in responding to a request for assistance from the Department of Social and Family Affairs.

The case also underlines that each Government Department is a Data Controller in its own right - Government is not a universal Data Controller- and there are mechanisms in place in Social Welfare and other Laws for the exchange of personal data, as necessary. I liken this to the bulkheads in a ship, so that data given for a particular purpose is compartmentalised and may not be used for other purposes without the consent of the citizen or without a statutory basis. This is the key principle in my Guidelines for the operation of E-Government and the REACH project, which I published in my Annual Report for 2000

Case Study 9

Details of other bank account holders of the same name, supplied in response to access request-inadequate response to customer-security procedures-lack of awareness at branch level of data protection

An individual complained to my Office in relation to her bank account as she was concerned about the accuracy and security of the information held and the potential disclosure of her details to other account holders, as there appeared to be confusion regarding her account and that of another account holder of the same name. She informed me that though she had complained to the institution concerned she had encountered difficulty in having the matter resolved. She was advised by my Office to make an access request, under section 4 of the Act, to this major banking group in order to establish what personal data was held about her on computer.

The bank's initial response to her access request comprised a copy of her data from the particular branch to which she had sent the request, and advised that if she wished to obtain personal details from other areas of the bank, she should write to the offices concerned, enclosing a separate fee with each request. It included a listing of the bank's registrations relating to the Public Register of data controllers that is held in my office.

It then transpired that her personal details as supplied by the Bank, contained a number of inaccuracies, viz. accounts at two other locations, neither of which related to her personally; the date of opening of the account, her marital status, her occupation and credit card details were incorrect ; details showed her as having a mortgage which was not the case. She had obtained this information by supplying to her branch in Dublin her name, address and ATM card number only. She was justifiably concerned that her data and that of other customers was being inappropriately disclosed and not kept in a secure manner.

her personal details as supplied by the Bank, contained a number of inaccuracies,

My Office contacted the bank but the investigation encountered considerable difficulty in obtaining an adequate response, as there did not appear to be anybody designated with responsibility to co-ordinate the provision of information in response to the access request. **There also appeared to be a distinct lack of awareness and appreciation of data protection requirements amongst management and staff.** Eventually, my Office contacted the Group Compliance Officer. Later my Office was informed that

"Our processing system endeavours to match customers across branches to highlight their entire relationship with the Bank. An error occurred in our system, either human or technical, whereby the customer's account number was matched to an account in the name of (same customer name) in two other (named) branches, even though they did not meet the required matching criteria. The accounts in both these branches had different account numbers. This was an unfortunate error that should not have happened. We have amended the process with regard to matching customers' accounts whereby the criteria for matching has been expanded considerably".

I concluded that important bank account details were not maintained in an accurate and up-to-date fashion and this was highly unsatisfactory from a data protection perspective. It also raised questions about the security of customer's accounts and improper disclosure of data. I noted the bank's commitment to expand considerably the criteria for matching, which should ensure that a recurrence of this incident is avoided. I also noted that the Bank was now very much aware of its responsibilities regarding the protection of personal data.

I informed the bank also that many data subjects making access requests might not necessarily be familiar with the requirements of the Act.

Accordingly, I suggested that data subjects be advised in plain language of the procedures in operation for accessing their data in other branches of the organisation as I considered that improvements were necessary in the letter that issued to the complainant.

In general I receive great co-operation from the main financial institutions. While this was a very serious case, I trust it was an isolated incident.

Case Study 10

Aer Rianta- inappropriate Use of the Personal Public Service Number (PPSN)

My office received complaints from a number of taxi drivers who had been operating from Dublin Airport for many years. Their complaints related to the Application Form issued by Aer Rianta for a permit to operate a taxi service from Dublin Airport, which asked interalia for the applicants' Personal Public Service Number (PPSN).

I contacted Aer Rianta and informed it that only public bodies that are designated under the Social Welfare Acts may request a person's PPSN. **As Aer Rianta are not a specified body under the Social Welfare Acts, they therefore had no authority to seek the PPSN.** Indeed, it is an offence under the Acts to do so. Aer Rianta immediately agreed to omit the request for the PPSN from their form.

I am particularly concerned to ensure that only those bodies that are specifically authorised by the Social Welfare Acts to use the PPSN do so as otherwise it could be used as a national identity number by the "backdoor". I liaised with the Department of Social and Family Affairs on this matter and the code of conduct and the publicity campaign they initiated during 2002 should bring clarity to the circumstances where the PPSN can and cannot be used. In Appendix 3 I refer to this general area in greater detail.

only those bodies that are specifically authorised by the Social Welfare Acts to use the PPSN can use it as otherwise it could become a national identity number by the "backdoor"

Case Study 11

Pharmacist - disclosure of sensitive prescription information - notifiable diseases and public health interests - issue of consent

A pharmacist contacted my Office seeking advice in relation to correspondence he had received from the Director of Public Health, Eastern Health Authority regarding a proposed scheme for pharmacists to assist in the surveillance of Tuberculosis. Pharmacists were asked to submit a form which detailed personal information of patients using anti-tuberculosis therapy prescriptions. The pharmacist was concerned that while the objectives of the proposal were well intentioned, he should not disclose sensitive information he held in trust without patient consent.

I contacted the Director of Public Health to establish whether this personal information had been fairly obtained as required under section 2 of the Data Protection Act. The Director of Public Health explained that one of his functions in relation to his duties as Medical Officer of Health relates to the surveillance and control of infectious diseases. Tuberculosis is a notifiable disease. There was significant public health concerns in relation to tuberculosis and the Department of Health, therefore, had instructed Directors of Public Health to seek such information from pharmacies.

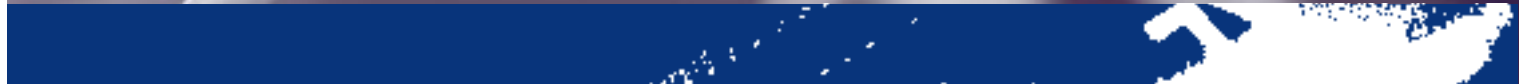
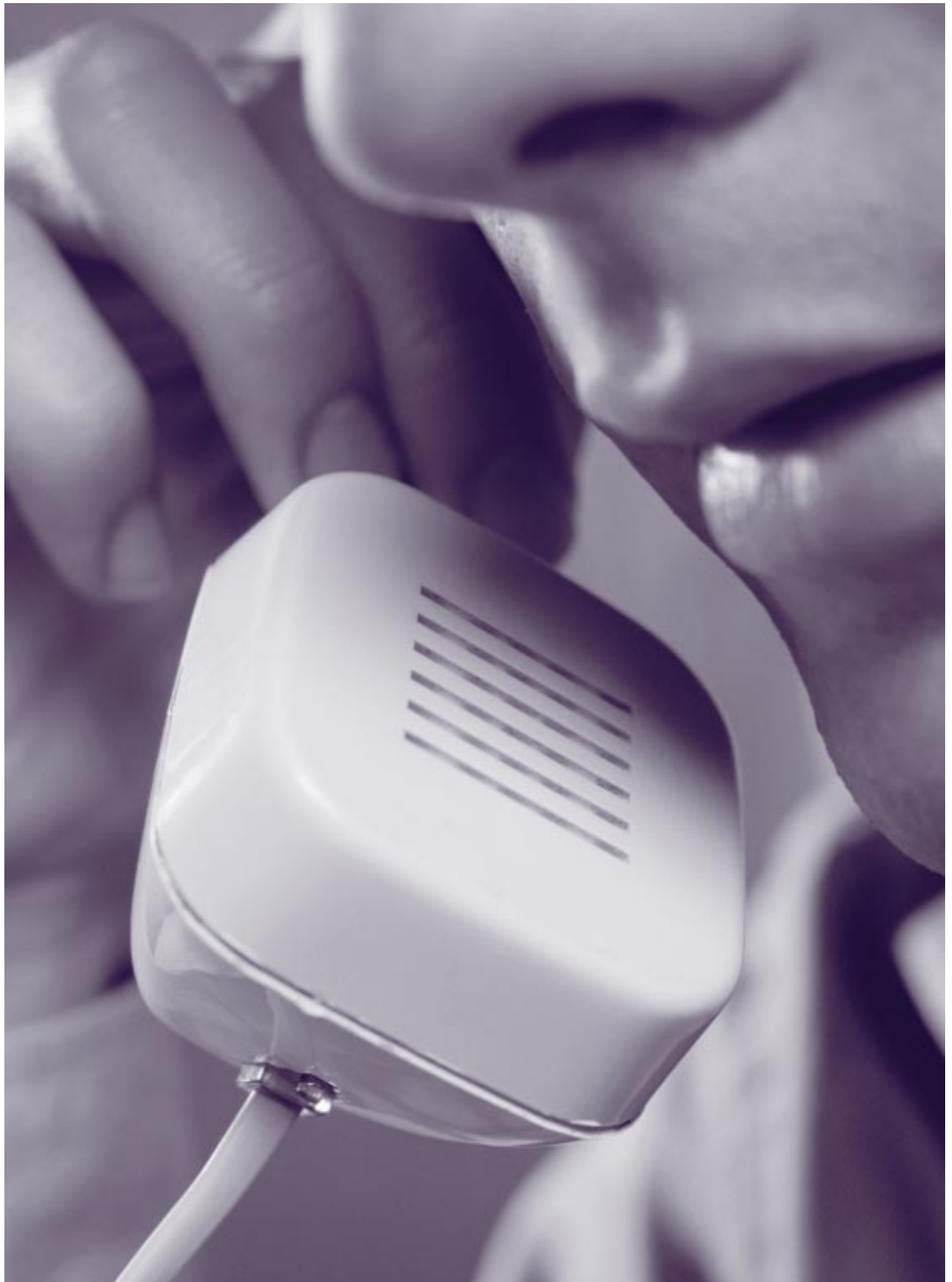
Having considered this response I contacted the Secretary General of the Department of Health and Children. I drew his attention to sections 11 and 14 of the Infectious Diseases Regulations 1981 (the statutory basis for reporting notifiable diseases) which provide that the responsibility to notify the Health Authority of an infectious disease falls on a doctor, not on a pharmacist. I assured him that I understand the importance from a public health perspective of having a reliable tuberculosis reporting system in place but, as Commissioner, I must ensure that such a reporting system respects the provisions of data protection law. I questioned why it was necessary to require pharmacists to notify Health Authorities of prescriptions - only doctors can issue a prescription and they have a statutory obligation to report an

incidence of a notifiable disease. I pointed out that such reporting by a doctor is covered by section 8(e) of the Data Protection Act, 1988 which lifts the restriction on disclosure if it is "required by or under any enactment or by a rule of law or order of a court". However, there was no statutory basis for reporting by pharmacists of notifiable diseases.

The Department of Health and Children informed me that reporting by pharmacists was introduced following a report of a Working Party on Tuberculosis in 1996 so as to enhance the tuberculosis surveillance system and ensure that appropriate contact tracing could be achieved. The Department, having considered the issues raised by me, decided that the reporting of this information by pharmacists should cease and wrote to each Director of Public Health informing them of the situation and advising them to notify all pharmacists in their functional area.

I was pleased that the Department took appropriate steps to address the issues involved in this case. "Fair obtaining" and **fairness and transparency require that personal details obtained for prescription purposes cannot be subsequently used for other purposes without express consent or, if there is a real public health need, a clear statutory basis.**

understand the importance from a public health perspective of having a reliable tuberculosis reporting system in place but, as Commissioner, I must ensure that such a reporting system respects the provisions of data protection law



Appendices

Appendix 1

Statement by the Data Protection Commissioner at the Forum on the Retention of Communications Traffic Data on 24 February 2003

I very much welcome this forum and I compliment Minister McDowell for hosting it as it is necessary that an informed debate takes place on this important matter. Let me say at the outset that as Data Protection Commissioner I will be supportive of measures that are demonstrably necessary to protect against crime or terrorism but such measures must be proportionate and have regard to the human right to privacy. The purpose of today's forum is to analyze the parameters in which communications companies can retain communications traffic data so that security services can have access to such data while respecting our privacy rights.

So what is traffic data? Traffic data in the communications field refers to the data that is created by your phone company (Telco) or Internet service provider (ISP) when you make a phone call, go on the Internet or send e-mail. It is necessary for billing purposes and you are aware of its contents if you get an itemized bill. Traffic data reveals huge amounts about one's private life. They are your electronic footprints but unlike the physical fingerprints you leave around you in the real world, they are recorded. For landline phone calls it can reveal the number you dialed, the duration of the call and the time of the call. Traffic data also includes a record of the location of the cell phone in question as it moves about from cell to cell. For this reason, traffic data generated by mobile calls is far more personal and revealing. In relation to the Internet, traffic data would encompass the e-mail addresses on all correspondence to and from the subscriber, a record of date, time, and size of message as well as other transmission details but hopefully excluding message subject and content. It would also encompass a record of every login session, every web page visited and read, every search term entered, every file downloaded, every purchase made, and so forth - in short, virtually the entirety of one's online "session" but hopefully excluding the content of e-mail messages.

In the ideal world once the bill is paid such data should be deleted though aggregate or anonymised detail can be held. Of course it is personal data and communications whether by post, phone or e-mail are meant to be confidential unless otherwise regulated by law. Because most people put an important privacy value on their communications

interception of or access to calls for law enforcement agencies is strictly regulated under the 1983 /1993 Postal and Telecommunications Services Acts and the 1988 Data Protection Act.

Are there privacy concerns? The retention of private communications, beyond the limited time necessary for billing purposes, therefore, is a significant measure in data protection terms. I do not doubt or question that there are extremely good law enforcement reasons for wanting such data to be retained for a longer period. However, if you can no longer feel secure that your telephone, web surfing and electronic communications are in fact private, then that signals a major change in the nature of the society in which we are living. Traffic data, if it is not securely controlled, could be used

- *as a source of great assistance to marketers including telcos and ISPs*
- *as a way of profiling your habits*
- *to monitor your movements by reference to location of call as an information source and /or to snoop on you if necessary*
- *to make wrong assumptions about your personal behavior*
- *to blackmail you perhaps if the communication service provider did not have adequate data security to provide against the potential for unlawful access by hackers and others*
- *as a means of surveillance on every citizen just in case they did wrong.*

It could therefore be easily abused unless stringent safeguards are in place. Unlike other forms of personal data as I have indicated traffic data can reveal very easily who you are communicating with and where you are in your normal private life even when there is no criminal activity of any sort contemplated or being carried out by you. In effect

- *would we avail of the phone or Internet if any of the foregoing was to be the norm and we were not clearly informed about them when we signed up to the service?*

Appendices - Appendix 1

- *would we be concerned if an ISP or the security service without just and legitimate cause read our emails?*
- *how can the legislation be framed to restrict access to law enforcement purposes only?*
- *as a democratic society would we be happy to forego some of our human rights to privacy in the absence of strict and proportionate measures to limit that right?*
- *do we want to live in a "surveillance society" where our normal activities could be routinely monitored and kept for inspection by the security services or what should the balance be?*
- *does the state want to keep data on everyone just in case we might become a criminal or does the state wish to treat us all as criminals?*

Therefore today we are considering how long telcos and ISPs should routinely retain traffic data for security or law enforcement access purposes and the challenges this may pose for me in my role as Data Protection Commissioner and ultimately for every citizen. That is why this forum is very important.

What is the importance of Privacy? Privacy is one of the "unenumerated rights" of our Constitution as established in case law by Supreme Court judgments. May I also quote from the Law Reform Commission 1998 Report on Privacy, Surveillance and the Interception of Telecommunications?

"Privacy is not merely instrumental to the achievement of other goals but is a basic human right that applies to all persons in virtue of their status as human beings. It is not possible to overstate just how fundamental privacy is in a civilized legal system."

What are the Data Protection angles therefore?

Section 2(1)(c)(i) of the Data Protection Act, 1988 provides that data controllers shall keep personal data only for one or more specified and lawful purposes. Section 2(1)(c)(iv) provides that personal data shall not be kept longer than necessary for that purpose or those purposes. It is legitimate for telcos and ISPs to process personal data for billing purposes. In principle, there seems to be no reason why a telco or

an ISP should retain billing data for any significant period of time after a particular bill has been settled. A short retention period, to allow for subsequent queries to be dealt with, would not appear unreasonable. It would also be legitimate for a telco or an ISP to retain personal data for longer periods in particular cases where a dispute has arisen regarding a bill, or where the telco has reasonable grounds to suspect that such a dispute may arise. However, it would be contrary to the Act to routinely retain billing data in all cases for a long period of time, irrespective of whether the bill has been settled, or of whether there is any reason to believe that a settled bill will subsequently be challenged. Apart from being retained longer than necessary, such data would appear to be "irrelevant and excessive", contrary to section 2(1)(c)(iii) of the Act. This then was my basis for demanding during 2001 that in line with the 1988 Act and EU directives traffic data, in general, should be routinely kept for a maximum period of six months- a position since formally adopted by the EU Data Protection Commissioners and the EU Commission.

As regards the current legal position I made an order, in January 2001, requiring telcos and ISPs to register with my Office. During the registration process I discovered that all traffic data for telcos was being routinely retained for a period of six years, the rationale being that it was necessary to do so in case a claim arose under the Statute of Limitations. I found it difficult to accept this reasoning and pressed for the six-month retention period to be the norm as outlined earlier. While this period was eventually acceptable to most of the telcos and ISPs it raised legitimate concerns in the Department of Justice regarding access for security and crime investigations. Following discussions with me the Department indicated that a retention period of three years, rather than the then six years, was necessary for security purposes for telcos. While I respected their view I consider that a maximum period of three years does not strike the correct balance. The Department however took my concerns to Government who decided in March 2002 that the Minister for Public Enterprise should issue Directions under s110 (1) of the Postal and Telecommunications Services Act, 1983, requiring telcos to retain detailed non-

Appendices - Appendix 1

anonymous traffic data for a three-year period, for the purpose of facilitating requests from An Garda Síochána and from the Defence Forces under sections 98A and 98B of the 1983 Act, as inserted by the section 13 of the Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993. The direction was issued in April 2002 to telcos. This measure was intended to be a temporary 'holding measure' pending the introduction of substantive legislation to this effect. The legislative process is now being finalised but I understand that ISPs could be included in the legislation also. While I was very unhappy with this approach I am much happier that the process has now been brought into the open for public debate.

EU law on the retention of telecommunication traffic data is regulated by Directive 97/66 which was transposed into Irish law on 8 May 2002-this is being replaced by Directive 2002/58, to be transposed by October 2003. Directive 2002/58 has not made significant changes to the existing provisions of retention of traffic data as it extends its scope to the more general context of electronic communications. Article 6 of Directive 97/66 provides that traffic data can be retained until the bill is paid while Article 14 of the Directive (Article 15 of Directive 2002/58) also provides that retention of traffic data for purposes of law enforcement should meet strict conditions i.e. in each case only for a limited period and where necessary, appropriate and proportionate in a democratic society.

Let me now address the matter of law enforcement access to traffic data and data protection. I, of course, recognise that privacy rights are in no sense absolute and must constantly be balanced against other competing interests not least the right to freedom of expression or society's right to be made aware of particular information which an individual might prefer to remain hidden. In my view the issues of public policy that need to be balanced are so delicate as to require fine tuning in stand alone legislation for particular serious issues. When a communications data controller is making disclosure of billing or traffic data to a law enforcement agency then it can rely on the provisions of Section 8(b) or (e) of the Data Protection Act which provide that

" Any restrictions in this Act on the disclosure of personal data do not apply if the disclosure is

(b) 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,

(e) required by or under any enactment or by a rule of law or order of court

(As regards security of the state this is covered under Section 8(a)). In my opinion, section 8 is permissive in that it lifts restrictions on the disclosure of personal data by a data controller, which would otherwise apply if none of the conditions specified in section 8 were met. Section 8(b) does not oblige a data controller to disclose personal data to anybody regardless of whether or not any of those conditions have been met. Furthermore I am of the opinion, that if section 8(b) is to be relied on it has to be established that there is a substantial risk rather than a mere chance that in a particular case at least one of the purposes mentioned (in 8(b)) would be noticeably damaged by the data controller's failure to provide the information sought. In other words, the prejudice test has to be clearly undertaken before any data can be disclosed or indeed requested. This is why any request by the law enforcement agencies to telcos or ISPs for access to traffic data has to be made by an officer not below the rank of Chief Superintendent or a Colonel in line with the terms of the 1983 and 1993 Postal and Telecommunications Acts.

I will now comment on **my role as Data Protection Commissioner**. I am independent in the exercise of my functions as a creature of the 1988 law passed by the Oireachtas. Because the Oireachtas has created me thus I am not a framer of legislation but in general Departments, when matters concerning data protection arise in any draft legislation or when schemes are being introduced, seek my observations. My main obligations under the law are to ensure that the privacy rights people are entitled to and the obligations placed on data controllers are fully

Appendices - Appendix 1

respected. Data protection law is not a barrier to law enforcement agencies carrying out their difficult tasks but it tries to strike a reasonable and proportionate balance between personal privacy rights and other demands placed on any democratic government. I believe it appropriate to reiterate that I am conscious of the sensitive issues of security, including national security. The precise content of the legislation to be introduced in this regard is ultimately a matter for Government subject to enactment by the Oireachtas and hopefully after careful consideration of my views on the matter and those expressed at this forum.

So what is my overall view on the retention period? Data protection law in this country is based on the principles outlined in the Council of Europe convention and in EU directives, which this country has implemented. In my view and in the view of my EU and other Privacy Commissioners where traffic data are to be retained in specific cases for security purposes

- *the traffic data involved has to be clearly defined and the burden of proof that privacy invasive measures are necessary must always be on those who claim that some new intrusion or limitation on privacy is necessary.*
- *it must be demonstrably necessary in order to meet some specific need*
- *it must be demonstrably likely to be effective in achieving its intended purpose i.e. it must be likely to actually make us significantly safer, not just make us feel safer;*
- *the intrusion on privacy must be proportional to the security benefit to be derived; and*
- *it must be demonstrable that no other, less privacy-intrusive, measure would suffice to achieve the same purpose.*

The European Union Data Protection Commissioners have also noted with concern that in the third pillar of the EU, proposals are being considered which would result in the mandatory systematic retention of traffic data concerning all kinds of telecommunication for a period of one year or more, in order to permit possible access by law enforcement and security

bodies. They have expressed grave doubts as to the legitimacy and legality of such broad measures and stated that systematic retention of all kinds of traffic data for a period of one year or more would be clearly disproportionate and therefore unacceptable in any case. They also drew attention to the excessive costs that would be involved for the telco and Internet industry, as well as to the absence of such measures in the United States. Finally the European Data Protection Commissioners have also repeatedly emphasized that such retention would be an improper invasion of the fundamental rights guaranteed to individuals by Article 8 of the European Convention on Human Rights

In conclusion you will appreciate this is a sensitive and complex issue for everyone where difficult choices have to be made. I welcome the measures to monitor this area by a judicial oversight and I accept that traffic data can be of valuable assistance to law enforcement agencies in particular instances. Data protection law is not a barrier to law enforcement agencies carrying out their difficult tasks but it tries to strike a reasonable balance between personal privacy rights and other demands placed on any democratic government. The privacy implications of traffic data retention are further compounded by the involvement of neutral third parties, i.e., the communication service provider, with all that this implies for data security and the potential for unlawful access by hackers and others. While I can well appreciate the arguments put forward in support of the systematic retention period of three years I remain to be convinced that a three-year retention period is necessary for the Gardai, the Defence Forces and ultimately the state to carry out their delicate and responsible work. Therefore a balance has to be struck. To strike the correct balance certain questions need to be raised and answered. I pose the following questions

- **have a significant number of requests been made for traffic data held for longer than six months or twelve months?**
- **how vital is traffic data to detecting crime?**
- **how valuable is traffic data in the detection of crime overall i.e. what % of solved serious crime is dependant on access to traffic data?**

Appendices - Appendix 1

- **if we are being asked to sacrifice our privacy we must have details about what we get in return. Once privacy rights are surrendered they may be hard to recover. We should therefore surrender these rights reluctantly, on the basis of convincing arguments and facts about other interests of society?**
- **what level of proof of suspected wrongdoing would have to be available to a telco or ISP or a judge in order to enable access to the data. Are we talking about crime detection, intelligence, specific investigations or a store of data relating to suspicious activity?**
- **will it be possible to ensure that access will only be allowed for security purposes or crime?**
- **will this type of legislation have a “sunset provision” so that the Oireachtas can review its appropriateness after a reasonable time period?**

It is a matter for the Oireachtas but I would ask you to reflect on the communiqué issued by over 50 Data Protection Commissioners following their annual conference in Cardiff in September 2002, which stated

“ The Commissioners agreed that whilst there is the need to protect society from the outrages of 9/11 the reactions in many countries may have gone beyond a measured response to the terrorist threat with serious implications for personal privacy. The Commissioners agreed that the need to safeguard personal privacy in such developments remains an essential task for the worldwide data protection community. Unless an approach is taken by Governments which correctly weighs data protection and privacy concerns there is a real danger that they will start to undermine the very fundamental freedoms they are seeking to protect”.

I look forward to the Minister bringing forward new legislation to address matters of importance that he and I are concerned with. I have no doubt but that the Oireachtas will fully debate these concerns when considering this matter and will address it by enacting legislation at an early date.

Appendix 2

Market Research Survey on Awareness of Data Protection

Basis for Survey

I considered it necessary to conduct a public survey during 2002 - a previous one was carried out during 1997. In order to maximise the effectiveness of the Office's operations in terms of addressing the concerns and meeting the needs of the public, it was decided to undertake research, amongst the general public, with the following key objectives:

- To measure the level of public awareness of data protection and privacy issues.
- To understand the extent to which the public is concerned with the protection of their privacy.
- To measure the degree of importance attached to privacy in respect of various items of private or personal information.
- To assess overall awareness of the Office of the Data Protection Commissioner.
- Whether the promotional campaigns of my Office needed to be refocused or increased in the light of current developments in data protection including the new Data Protection legislation coming into force during 2003. In general over the years the Office's limited promotional campaigns have been targeted specifically at the business area and not at people.

I also intend to carry out a similar type survey in the business and public sector areas in the future.

Methodology

A market research company, Millward Brown IMS, selected by tender carried out the survey. A sample of 1,203 respondents, aged 15+, were interviewed on the Millward Brown IMS Omnibus Survey. This survey was designed to be representative (in terms of age, sex, social class, region and area) of the adult population aged 15 and over living in Ireland. All respondents were interviewed face to face, in their own homes by Millward Brown IMS interviewers. Fieldwork was conducted between 24th September and 4th October 2002. In order to maintain

comparability with previous research undertaken in October 1997, the findings set out below are based only on those aged 18 years or over (1,098 respondents).

Summary of Survey- Public anxiety about personal privacy linked to 'Trust Deficit' while awareness of the Data Protection Commissioner's Office is unsatisfactory

Irish people are growing increasingly concerned about the erosion of their personal privacy. Intrusive business practices, fears about Internet privacy, and a lack of information about Government initiatives have contributed to a "trust deficit" that could undermine Ireland's progress towards e-commerce. While 39% of those surveyed reported that they had heard of the Office (compared to 25% in 1997) nevertheless only 8% (2% in 1997) spontaneously mentioned the Office as a conduit for complaints about invasion of privacy- the Gardai being the most likely first port of call mentioned, followed by the Ombudsman. Considering the limited promotional campaigns carried out to date, the finding was not unexpected.

Key Findings

The key findings are:

- Irish people value their privacy highly, ranking it higher even than issues such as consumer protection, ethics in public office, and equality in the workplace. Only crime prevention was given a similarly high priority by the public.
- Financial records have a marginally higher privacy value than medical records.
- Three out of four Irish adults believe that businesses regularly encroach on our privacy. Irish people share a similar mistrust of Government agencies – just over half of adults trust Government agencies to deal with personal details in a fair and proper manner, with one in four expressing distrust.

Appendices - Appendix 2

- People feel more insecure about the Internet than in the past. Most people (56%) agree that 'if you use the internet, your privacy is threatened', compared with 37% in a 1997 survey. The proportion that 'strongly agrees' with this statement has doubled from 14% to 28%.
- Most people prefer not to receive unsolicited direct marketing. While many people tend to be somewhat indifferent to direct mailings to the home, people are more firmly opposed to receiving unsolicited phone calls at home, and to receiving unsolicited e-mails and SMS messages.
- Comparing these results with a similar 1997 survey, peoples' anxieties about intrusions into their privacy have increased. Expressions of unease about business practices and about Internet use have all increased significantly over the period.
- While 39% of those surveyed reported that they had heard of the Office of the Data Protection Commissioner (compared to 25% in 1997) only 8% (2% in 1997) spontaneously mentioned the Office as a conduit for complaints about invasion of privacy.
- There is a large element of uncertainty among the general public as to what exactly their data protection rights are.
- Middle class people and young adults are the most likely to be aware of the Data Protection Commissioner's Office while people over 65, working class people and farmers are least aware of their data protection rights.
- Only one in three adults had assimilated developments in relation to the PPSN.

Response to Survey - Privacy-Proofing initiatives are needed while my Office has to make people more aware of their rights

The survey indicates that action must be taken at various levels.

- As the information society proceeds apace, public unease about new technologies needs to be firmly laid to rest. This survey shows that public anxieties are, if anything, on the increase. The Government and the business community, as well as my Office, have a role to play in addressing these fears.
- While Data Protection Law is there to provide the assurances that the public demand I urge the business community and the Government to build privacy-proofing initiatives into the way they interact with the public. Information, transparency and consent are the touchstones of good practice in both the public and private sectors, and the success of e-business will ultimately depend upon public credibility.
- For my part there is a greater need to make ordinary people more aware of their rights as the level of knowledge about my role is not satisfactory. I intend to carry out an awareness media campaign focused on personal rights during 2003. I will be re-doubling my enforcement efforts in 2003, to ensure that people's legal rights in this area are respected by launching privacy audits and exercising a range of new powers open to me under the new Data Protection (Amendment) Act, 2003.

DETAILED RESULTS OF THE SURVEY

1. Irish People Value their Privacy

The survey shows that Irish people place a high value on their right to privacy with a positive rating by 98% of those surveyed. "Privacy of personal information" ranks higher even than the "protection of consumer rights," or "ethics in public office". Only "crime prevention" received a similarly high rating by the public.

Appendices - Appendix 2

	Important	Very important
Crime Prevention	15%	84%
Personal Privacy	17%	81%
Consumer protection	20%	76%
Workplace equality	19%	75%
Ethics in public office	22%	71%

2. Financial Records More Sensitive Than Medical Records

Irish people place a higher privacy value on their personal financial records than on their medical records. 77% of adults rated their “financial history” as “very important” (with a further 18% rating it as “important”), compared with a 72% “very important” rating for “medical records” (with a further 21% “important” rating). Other items of personal information with strong privacy ratings were credit card details (70% very important, 14% important), and the PPS Number (60% very important, 25% important). The personal telephone number was rated “very important” by 51% of adults, and as “important” by a further 28%. Other personal details received lower privacy ratings: date of birth (37% very important, 22% important), and marital status (31% very important, 19% important).

3. Businesses need to be More Privacy Friendly

Three out of four adults believe that businesses are encroaching upon personal privacy. 76% of people agreed with the statement that “businesses regularly want to know more about me than they need to” – a significant increase since 1997, when the comparable figure was 60%. More worryingly, the proportion of people who agree strongly with this statement has more than doubled from 19% in 1997 to 41% now. This negative perception of business prevailed across all age and social class cohorts, with the professional/managerial (AB) group (85%) and married men (84%) particularly vociferous in this regard.

On the other hand, around half of adults (54%) tended to agree that they “trust businesses to use the information they have about me in a fair and proper manner.” One in every four (25%) actively disagreed with this statement, while the remaining one in five were either ambivalent or did not know. The most sceptical were men (30% disagreeing), AB’s (34%) and Dublin residents (34%).

Reaction to the notion that ‘it is worth giving up some privacy to enable businesses to provide better services’ was somewhat more polarised, with quite similar proportions of all adults either agreeing (43%) or disagreeing (37%) with this proposition. Looking across the demographic groups, the balance of opinion in favour of this statement was highest among those in the lowest socio-economic group (DE), and residents of Leinster (excluding Dublin) and Connaught/Ulster. Opposition tended to outweigh agreement among Dublin residents and single women.

4. Similar Mistrust of Government Agencies

Interestingly, the general public appeared no more trusting of government organisations and agencies than they were of businesses in relation to the proper use of their personal information. Overall, just over half of adults (52%) agreed to a greater or lesser extent that they ‘trust government organisations and agencies to use the information that they have about me in a fair and proper manner’. One in every four (26%) disagreed.

5. The Internet and Privacy

People’s fears of the Internet seem to have grown in the last number of years. 56% of adults now agree that ‘if you use the Internet your privacy is threatened’, compared with 37% in the 1997 survey, and the proportion that ‘strongly agree’ with this statement has doubled from 14% to 28%. Thus, although a similar proportion as in 1997 (23% now versus 27% then) remained uncertain (presumably through lack of knowledge and experience) of the impact of the Internet on their privacy, these latest results show that Internet users have definitely

Appendices - Appendix 2

become more rather than less chary in the intervening period of the risks to their privacy.

6. People Are Hostile to Intrusive Direct Marketing

Most people tended to be opposed to, rather than in favour of, unsolicited direct marketing. Predictably, because of its more immediately intrusive nature, resistance tended to be highest to direct marketing attempts over the home telephone, with more than one in every three adults (36%) describing themselves as 'very unhappy' about this selling approach and three in five overall (60%) opposed to some extent. Antipathy to this form of direct marketing was highest among ABC1's (67%) and Dublin (67%) and Munster (70%) residents.

As regards direct marketing by e-mail or over the Internet - this question was relevant for only two out of three respondents - the level of discontent was high, with 55% opposed to receiving communications this way. Middle class (ABC1) and older respondents (25 years and upwards) were the most resistant.

Focusing on those who gave an opinion about direct marketing messages via SMS/text to mobile phones, over half (54%) pronounced themselves unhappy with this type of communication. One in every four was unconcerned one way or the other and one in eight were happy to receive such communications. Young people (18 – 24 years) who tend to be the most assiduous users of mobile phones, appeared less concerned, while those in the 25 – 49 year span were the most likely to reject this method of direct marketing, as also were middle class (ABC1) respondents and Dublin and Munster residents.

Although a substantial proportion (48%) were also opposed to some degree to direct marketing through the post, this medium was also the most likely to elicit indifference - 'don't mind one way or the other' (32%). Consequently, relative to the other forms of communication measured in the survey, direct marketing communication through the post is perhaps less contentious or intrusive. The oldest age group (65+ years) appeared the unhappiest about this

type of direct marketing. Regionally, Dublin and Munster residents were also the most strongly opposed, perhaps reflecting a proliferation of 'junk mail' in more urbanized areas.

7. Awareness of Data Protection Commissioner's Office

In order to assess spontaneous awareness of the role of the Office of the Data Protection Commissioner, respondents were asked where they would go if they wished to make a complaint about invasion of their privacy in terms of personal information. Their initial unprompted responses revealed that the Gardai would be sought by 24%, the Ombudsman by 14% as against 8% for my Office- in 1997 54% would have contacted the Gardai, 3% the Ombudsman while only 2% would have contacted this Office. Across the socio-demographic cohorts, middle class (ABC1) respondents and residents of Dublin and Leinster were somewhat more likely than average to mention the Data Protection Commissioner. Interestingly 26% in the higher socio economic (AB) group mentioned the Office of the Ombudsman, ranking it ahead of all other sources. Lower down the socio-economic scale, blue-collar respondents were more likely than average to mention the Gardai.

When asked specifically whether they had ever heard of the Data Protection Commissioner 39% reported that they had (compared to 26% in 1997) while 51% said they had not. One in every ten did not know. Awareness increased to 57% among middle class adults (ABC1s) and was even higher (64%) for the professional/managerial group. Young adults in the 25 – 34 year age group also showed an above average awareness of the Data Protection Commissioner, as also did those resident in Connaught/Ulster. Those least likely to be aware were the 65+ age group (24%), the unskilled working class group (23%) and members of the farming community (28%). As these are the groups that are in a sense the most 'at risk' through lack of knowledge, it will be important to give these specific focus in any future promotional and educational campaigns emanating from the Office.

Appendices - Appendix 2

8. Perceptions of Legal Entitlements in Relation to Privacy Information

Various statements concerning their legal rights to information were read out to respondents and they were asked to indicate which they believed they were entitled to, or not. In order to assess the extent to which people had a genuine grasp of their entitlements, two 'dummy' scenarios were included in the list of situations, namely 'to be given a list of all organisations that hold personal data about you' and 'to have any of your medical records deleted'.

Peoples' perceptions of their legal entitlements in relation to each of the scenarios suggest that the general public believes the legal obligations of organisations regarding personal information are more extensive than they are in reality. For example, approaching two in every three adults (64%) believe that they are entitled to be given a list of all organisations holding personal data about them and over two in five (42%) believe it is their right to have any of their medical records deleted. That so many should concur with these 'dummy' scenarios, suggests that there is probably a large element of uncertainty among the general public as to what exactly their entitlements are, and that their assessment of each of the statements presented to them is based as much on guesswork and perhaps logic, as on informed judgment.

Those aware of the Data Protection Commissioner (39% of all adults) tended to have a heightened perception of their entitlements regarding the management of their personal information, in relation to both the actual and spurious statements, although admittedly they were less credulous regarding their entitlement to have any of their medical records deleted than they were in relation to the other statements measured. Generally speaking, those most likely to claim entitlement for each of the genuine scenarios tend to be in the 25 – 34 and 35 – 49 year age groups, middle class (ABC1), and resident in Dublin. Uncertainty regarding their entitlements (don't know/no opinion) was more likely to be a feature of older adults (65+) years, those at the lower end of the socio economic scale (DE), members of the farming community and Munster residents.

9. Awareness of the Personal Public Service Number (PPSN)

Awareness of the PPSN was relatively low, with just one in three of all adults claiming to know about its introduction, and its function as a unique identifier number to enable Government organisations and agencies to link and transfer personal information. Demographically, awareness of the PPSN peaked in the professional/managerial sector (AB), and was also above average for white-collar respondents, those in the 25 – 49 year age group and residents of Connaught/Ulster. Conversely, those least likely to have heard of developments in this regard were the unskilled working class (DE), the oldest age group (65+ years) and Dublin residents. Predictably, those aware of the Data Protection Commissioner tended to be more aware of the PPSN.

Regardless of whether or not they had been actually aware of developments in relation to the PPSN, respondents were asked how they personally felt about government agencies and departments being able to link and transfer personal information via the PPSN. Reactions were quite polarised, with 26% of all adults in favour to at least some extent and a slightly higher 31% opposed. However, there also appeared to be a degree of ambivalence and uncertainty, with 16% overall claiming to be neither for nor against this development and more than one in four (27%) unable to form an opinion. In common with their higher level of awareness of developments in relation to the PPSN, middle class (ABC1) adults and residents of Connaught/Ulster were the most likely to react favourably, as also were those who were aware of the Data Protection Commissioner. Focusing on the one in three adults who actually claimed to know about developments in relation to the PPSN, the outcome was more positive, with more than twice as many (47%) in favour of the idea as opposed to it (21%). Based on this evidence, it may well be that, as people are made more familiar with the functions and capabilities of the PPSN, reaction will become more positive.

The subsequent publicity campaign in 2002 by the Department of Social and Family Affairs should improve perceptions of the PPSN.

Appendix 3

The PPSN as a Unique Personal Health Identifier Number

The Personal Public Service Number (PPSN) was introduced in the 1998 Social Welfare Act as the unique personal identifier for transactions between individuals and Government Departments and other agencies specified in the Social Welfare Acts. The PPSN replaced the Revenue and Social Insurance Number (RSI No.) that was only used in relation to transactions with Revenue and the Department of Social and Family Affairs. Legislation regulating the use of the PPSN provides that

- *The PPSN can be used either by the public bodies named in the Social Welfare Acts or by any person or body authorised by these public bodies to act on their behalf- a useful guide is published on the Department of Social and Family Affairs web site <http://portal.welfare.ie/ppsn/index.xml>.*
- *Any person who has a transaction with a public body e.g. an employer making Income Tax/PRSI returns on behalf of an employee can also use the PPSN.*
- *An Garda Síochána or the Defence Forces cannot use the PPSN for anyone other than their own members.*
- *While designated public bodies can only use the PPSN, equally it can only be used by such bodies for particular transactions and where the transaction relates to a public function of a public body. This is to ensure that the PPSN cannot be used for private or commercial transactions.*

Over the last year I have had ongoing discussions with the Department of Health and Children regarding their desires that the PPSN be used as a unique personal identifier for the health sector including the private health sector. A unique personal health identifier number is considered a vital part of its future Health Information Strategy. The principal reasons supporting the introduction of unique identification across all areas of the health services are to ensure that the most efficient and effective patient care is delivered and to provide assurance of patient safety. The Department feels that this cannot be achieved through the separation of “public” and “private” healthcare records. As data protection issues arise from this proposal I feel it appropriate to outline in this report concerns I have expressed to the Department.

Data protection law is no barrier to a proper functioning health service because it provides an assurance that in this delicate area peoples’ privacy rights are protected. In this regard data protection complements the confidentiality obligations of medical ethics. Accordingly I understand the necessity for a unique personal identifier in the context of the development of an Electronic Health Record and can see the attractiveness, from a health administrator’s perspective, of basing it on the PPSN. However this could ignore the fundamental purpose of the PPSN, which is a number established for specific public service purposes by legislation. There are fundamental data protection problems with a number that is established for one purpose being used for another purpose, including private sector purposes. I am also aware that in Ireland there can be overlap in the provision of both public and private health care but I have to be convinced that in circumstances where people are only availing of the “private” service that there is a “public” service element to it. I can further appreciate that information technology can be a key tool in reducing medical errors .

Notwithstanding the importance of the health area, the proposed extension of the use of the PPSN into the private health sector – unless it is proven that there is a necessary “public” element to that service-would potentially make it very difficult in the future to resist its use by other sectors, giving rise to the very real possibility that it could become a National Identification number by stealth. (In fact, during 2002, I had occasion to request a company (Case Study 10) to stop using the number and in this regard the Code of Practice published in 2002 by the Department of Social and Family Affairs and its subsequent publicity campaign are commended as they clearly outline the role of the PPSN.) This is a matter of substantial public policy with repercussions far beyond the Health Sector, affecting, as it would in a very real way, the relationship between the citizen, the State and the private sector. However I would have no difficulty with the introduction of a national identity number-with sufficient safeguards- if the Government, on the basis of specific stand-alone legislation being brought forward and properly debated by the Oireachtas, considered this necessary or desirable.

Appendices - **Appendix 3**

Furthermore the proposal could be characteristic of the phenomenon of "information and function creep", which is of general concern to me and many individuals and which has been observed in other countries, where a limited proposal is extended to purposes beyond those originally envisaged, with consequent implications for the privacy of citizens.

Irrespective of the outcome of this dialogue the more important issues going forward – when the issue of a central unique personal identifier for the health service is resolved - will be ensuring that peoples' privacy will not be eroded when delivering an effective and modern health care system. As patient information should only flow in parallel with patient treatment any computerised health identification information system will need interalia stringent security controls, "need to know" access provisions and detailed audit trails.

The Department has given my reservations serious consideration and I am confident that following our deliberations suitable solutions will be found in this delicate but necessary area. I am also appreciative of the efforts being made by the Department to meet my concerns.

Appendix 4

Extracts from the Strategy Statement and Business Plan 2003/4

Foreword from the Data Protection Commissioner

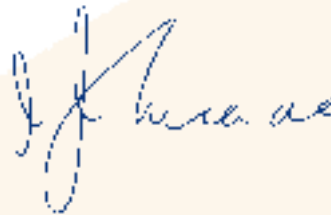
In launching our combined Strategy Statement and Business Plan for 2003/4, I wish to put on record my appreciation of the staff of the Office for their ongoing efforts in ensuring that the Data Protection Act, 1988 is administered in a fair and independent manner. Being an office that has many dealings with the public, with State organisations and with many large private concerns, it behoves us all to provide an efficient public service. In this document, we set out how we propose to work towards this in the eighteen months ahead.

The key principle of data protection is that living people should be able to control how personal information about them is used or at the very least to know how others use that information. Data Protection is a vital component of the information society and good data protection practices will help to foster public trust and contribute towards its success.

The staff themselves as part of the PMDS process mainly compiled this Strategy Statement and Business Plan. In the course of this, we reviewed our organisational structure to get maximum benefit from the additional resources recently assigned. By involving all staff in this wider consultative and management process, we aim to integrate PMDS more into our daily work and build on, and where appropriate improve, our level of service to the general public, to increase awareness of data protection amongst data subjects and data controllers and to be proactive in relation to compliance and enforcement activities; while at the same time ensuring that the Office continues to be sufficiently resourced to deliver its mandate.

In anticipation of the extra workload that will fall on the Office following the enactment of the Data Protection (Amendment) Bill, 2002 which is at present before the Oireachtas, our staff numbers were increased from 8 to 16 during the period of the last Strategy Statement and Business Plan for 2001/2002. I am grateful to the Department of Justice Equality and Law Reform for this. The current level of resources, taken with the remaining 5 posts which are due to be filled, should enable us to meet the challenges arising from the transposition of the EU Directive as well as the other new responsibilities arising in the "third pillar" of the EU which relate to police and judicial cooperation in criminal matters, including cooperation by customs authorities in this area viz. Europol, the Customs Information System, the Schengen Agreement, Eurodac and Eurojust. The Telecommunications Directive 97/66 was also transposed during 2002, while its replacement Electronic Communications Privacy Directive 2002/58 is due to be transposed by October, 2003. In addition the eCommerce Directive 2000/31 is to be transposed in the near future.

While we have made plans for our new responsibilities, and set definitive targets, these will require being under regular review during the early life of the new Law. That is why this Strategy Statement and Business plan is for 18 months only.



Joe Meade
Data Protection Commissioner

February 2003.

Strategy Statement

Our Role

Primary Responsibilities

The Office of the Data Protection Commissioner is established under the 1988 Data Protection Act, which was enacted in July 1988, and came into operation on 19 April 1989. The Act sets out the general principle that individuals should be in a position to control how computer data relating to them is used. "Data controllers" -- people or organisations holding information about individuals on computer -- must comply with certain standards in handling personal data, and individuals have certain rights.

The Data Protection Commissioner is responsible for upholding the rights of individuals as set out in the Act, and enforcing the obligations upon data controllers. The Commissioner is appointed by Government and is independent in the exercise of his or her functions. The Commissioner makes an annual report to both houses of the Oireachtas. Individuals who feel their rights are being infringed can complain to the Commissioner, who will investigate the matter, and take whatever steps may be necessary to resolve it.

The Commissioner also maintains a register, available for public inspection, giving general details about the data handling practices of many important data controllers, such as Government Departments and State-sector bodies, financial institutions, and any person or organisation who keeps sensitive types of personal data.

European Functions

In addition to his primary responsibilities, the Data Protection Commissioner also exercises functions arising from Ireland's commitments at European level.

Article 29 Working Party

- The Commissioner is a member of the Working Party on data protection established under Article 29 of EU Data Protection Directive 95/46/EC. This Working Party brings together all of the Data Protection Commissioners in the EU to discuss matters of common interest, and agree common positions on the application of the Directive.

Supervision of Europol

- The Commissioner is designated under the Europol Act, 1997 as the "national supervisory body" for Ireland for the purposes of the Europol Convention. This function involves monitoring the activities of An Garda Síochána in liaising with Europol Headquarters in The Hague, The Netherlands. The Commissioner is also a member of the Europol Joint Supervisory Body, which monitors Europol's operations to ensure that people's privacy rights are respected.

Other EU Initiatives

- EU Member States are also putting in place mechanisms to provide for cooperation by customs authorities (under the Customs Information System (CIS) Convention, 1995), by immigration authorities (under the Eurodac Regulation allowing for exchange of fingerprint information), through the Schengen Agreement, which allows for passport-free travel among participating Member States and for judicial and prosecuting co-operation under the Eurojust convention. All of these initiatives involve the maintenance of large databases with sensitive personal information, and therefore data protection safeguards are needed. The Data Protection Commissioner is the National Supervisory Body for the data protection elements of these initiatives and on the various European Supervisory Bodies.

Appendices - Appendix 4

Our Mission

To protect the individual's right to privacy by enabling people to know, and to exercise control over, how their personal information is used, in accordance with the Data Protection Act, 1988.

High-Level Goals

To maximise

- Peoples' ability to exercise their data protection rights
- Levels of compliance with data protection obligations

Analysis of our Environment

In pursuing our Mission and our High-level Goals, we must construct our strategy in line with the environment in which we operate. The constraints, challenges and opportunities we face are the key shapers of what we aim to deliver over our eighteen-month business planning period.

Strengths

Adaptability

- We are a small, flexible and adaptable organisation. This enables us to identify new and emerging priorities for action at an early stage.

Team Commitment and Capability

- Our tightly knit organisation has the capacity and the commitment to deal with any data protection issues that face us, in a principled, pragmatic and effective way.

Staff Resources

- Our office of sixteen people contains sufficient staff resources to tackle the day-to-day data protection issues that confront us. We are in a position to redeploy staff on a short-term basis to deal with newly emerging problems. A major challenge has been to integrate the new staff while retaining the tightly knit commitment that has been the hallmark of the Office.

Weaknesses

Expertise to deal with wide range of work

- While our staff numbers have increased by 100 per cent, we recognise that the wide range of technical and legal issues that confront us, plus our commitment to carry out privacy audits, present a major challenge. Staff training and data protection education of our staff will, therefore, be significant priorities for the year ahead.

Opportunities & Challenges

EU Directive and the Data Protection (Amendment) Bill, 2002

- The Directive and the Bill strengthen the privacy protections for individuals and assign more powers to this office. At the same time, adapting our organisation to the requirements of the Directive – both in terms of our internal expertise, and our capacity for action – is posing a challenge. To get the most out of our resources will be the most important challenge for us.

Appendices - Appendix 4

Education and Awareness

- Levels of awareness of data protection are low in Ireland, a fact borne out by the recent Awareness Study published by this Office. However, there is an increasing demand, in the context of the information age, for people to know more about their privacy rights. It is up to us to meet this demand: the enactment of the 2002 Bill, which will alter the existing data protection landscape, is both an opportunity and an enormous public education challenge.

The Internet

- With increasing adoption of the internet as a medium of communication, commerce and leisure, new specific threats to personal privacy are emerging. The fact that the information age in Ireland is still in its early growth stage allows us an opportunity to exercise a formative influence. On the other hand, unless we can act decisively in the near future, privacy-unfriendly internet practices could gain a momentum and achieve a de facto status that will be more difficult to displace. We aim to build on the work already done with the Internet Association of Ireland in regard to prominence being afforded to Privacy Policies on Websites.

E-Government

- The Government is committed to delivering public services over the Internet – “e-Government”. This initiative poses data protection challenges, which have been addressed in Guidelines published in our Annual Report for 2000. The Health area, in particular, raises sensitive issues, which we hope to address through Codes of Practice to be developed by experts in the various services. Through continued constructive participation with projects such as Reach, we can bring a positive influence to bear so that Data Protection will be seen as crucial to public confidence in such initiatives.

Key Ongoing Objectives

Customer Service Objectives

- To resolve complaints under the Data Protection Act, in accordance with the highest standards of customer service.
- To provide comprehensive, definitive and clear information and advice to our customers regarding data protection matters.
- To develop the registration process as a tool to empower individuals to have a full and meaningful understanding of how their personal information is processed.
- To take proactive measures to improve levels of compliance with data protection obligations.

Education and Awareness Objectives

- To increase levels of awareness among the public about their data protection rights and how to exercise these rights.
- To increase levels of awareness among persons processing personal information about their data protection obligations.

Organisational Objectives

- To perform our role and independent functions in a manner that is transparent and accountable.
- To develop the abilities, skills and competencies of our staff to contribute to the functions of the office, and to increase our capacity to develop our personal work satisfaction, our performance, and our careers.
- To strengthen and streamline internal administrative procedures.

International Objective

- To develop our ability to contribute in an effective way to international cooperation and to our international functions.

Business Plan

Objective 1:

To resolve complaints under the Data Protection Act, in accordance with the highest standards of customer service.

One of the key functions of the Office is to deal with complaints from members of the public. Clearly, where people feel so strongly about their data protection and privacy rights that they make a formal complaint to us, we must give this matter the highest priority. People do not complain unless they feel that they are not in a position to exercise control over their personal data –something that is at the heart of Our Mission. It is through complaints that the Office becomes aware of the ways in which Data Protection Law may be contravened by data controllers and decisions on complaints help to crystallise how the principles of the Act should be applied in practice. Since tackling complaints is our fundamental public service function, we must ensure that we treat such matters with the highest standards of customer service – including courtesy, timeliness and getting results. Our approach in this area will continue to be to seek to reach a mediated resolution of the problem at issue.

Key Deliverables

Timeliness

- 1.1 To address complaints as promptly as possible in order to facilitate their speedy and effective resolution; having regard to the varying complexity of some cases, which can have significant implications for time scales.

Effective Organisation

- 1.2 To maintain and develop an effective casework management system

Using IT effectively

- 1.3 To develop the IT system to facilitate the speedy and effective resolution of complaints.

Building our staff competencies

- 1.4 To develop the capacity of staff to deal with complaints in a speedy and effective manner

Objective 2:

To provide comprehensive, definitive and clear information and advice to our customers regarding data protection matters.

Our Mission requires that people should know their rights, as a first step to exercising these rights. Equally, data controllers must know their obligations before they can comply with them. Therefore, when people come to us for advice or information, they should receive a professional response. This means that our advice is –

- Comprehensive – we can answer any questions about data protection law
- Definitive – the advice we give is authoritative and reliable
- Clear – our advice is easy for people to understand and put into practice.

Key Deliverables

Telephone Service

- 2.1 To provide an efficient, effective and courteous telephone advice service

Prompt Written Advice

- 2.2 To respond to written requests for advice ordinarily within 28 days

Our Ability to Advise

- 2.3 To develop the capacity of staff to deal with written requests for advice in a speedy and effective manner

Appendices - Appendix 4

Objective 3:

To develop the registration process as a tool to empower individuals to have a full and meaningful understanding of how their personal information is processed.

The Data Protection Commissioner is charged under the Act with maintaining a register of certain data controllers and data processors. The purpose that underlies the registration system is to ensure that data processing takes place in an open and transparent manner. An effective registration system is therefore directly linked to the achievement of Our Mission, by “enabling people to know how their personal data is used”.

Key Deliverables

Meaningful and Informative Register Entries

- 3.1 To increase the usefulness of the public register by ensuring that register entries are more meaningful, informative and relevant

Compliance and enforcement

- 3.2 To maximise compliance with section 16 of the Act.

Accessibility

- 3.3 To maximise public access to register

Efficient Assessment of Applications

- 3.4 To increase efficiency of registration assessment procedures.

Efficient Administration

- 3.5 To maximise efficiency of the registration system

Objective 4:

To take proactive measures to improve levels of compliance with data protection obligations.

Protecting people's rights is an active mission for our Office, not a passive duty. To meet Our Mission effectively we must take positive steps to promote and to police data protection practice. The benefits of meeting this objective are two-fold:

- We serve the public interest by promoting a climate of good privacy practice; and
- By bringing the provisions of the law to bear upon wrongdoers, we send out a clear signal that the right to privacy is to be taken seriously as a fundamental human right.

Key Deliverables

Active Self-regulation

- 4.1 To encourage adoption of sectoral codes of practice and responsible self-regulation

Proactive Policing

- 4.2 To institute privacy audits

An Effective Prosecution Function

- 4.3 To refine and enhance the effectiveness of our prosecution procedures

Objective 5:

To increase levels of awareness among the public about their data protection rights and how to exercise these rights.

The first requirement in promoting people's privacy rights is that the people should have a full and in-depth appreciation of these rights. This is why Our Mission requires that people be “enabled to know, and to exercise control over, how their personal information is used”. Accordingly, spreading the news about data protection is a principal objective.

Appendices - Appendix 4

Key Deliverables

A Strategy for Awareness

- 5.1 Institute a strategy for promoting awareness of data protection rights and responsibilities

Objective 6:

To increase levels of awareness about data protection obligations among persons processing personal information.

Ignorance of data protection law is not an excuse for failure to comply – particularly given that the basic principles of data protection are matters of common sense and common courtesy. Nevertheless, we should ensure that the scope for accidental or casual breaches of the law is minimised, by promoting awareness of the law among data controllers.

Key Deliverables

Know Where We Stand

- 6.1 Determine levels of awareness regarding data protection rights and issues among data controllers and data processors

A Strategy for Awareness

- 6.2 Institute a strategy for promoting awareness of data protection responsibilities

Objective 7:

To perform our role and independent functions in a manner that is transparent and accountable.

This Office is established by law, and we must be seen to carry out our functions in a fair and independent manner. At the same time, we are public servants, and the requirements of accountability and transparency are essential if we are to retain the

confidence of the public.

Key Deliverables

Timely Accounts

- 7.1 To prepare annual financial accounts in a timely manner

Annual Report

- 7.2 To prepare a timely, concise and informative Annual Report

Transparency and Openness

- 7.3 To ensure that the efficiency and effectiveness of our operations are open to public scrutiny.

Objective 8:

To develop the abilities, skills and competencies of our staff to contribute to the functions of the office, and to increase our capacity to develop our personal work satisfaction, our performance, and our careers.

The quality of our service to the public is crucially dependent upon the capacity, the performance and the motivation of our staff. Moreover, we as an Office must show commitment to the development of our staff, if our staffs are to give commitment to the work of the Office. Therefore we must actively prioritise our staff development function in a tangible way.

Key Deliverables

Human Resource Management

- 8.1 To manage the human resource functions of the office

Training and Development

- 8.2 To support and encourage continued staff training and development, within the context of PMDS

Appendices - **Appendix 4**

Making PMDS happen

- 8.3** To incorporate the Performance Management and Development System as a core element of our business development strategy

Objective 9:

To strengthen and streamline our internal administrative procedures

To work effectively, our Office needs to have robust, reliable and efficient internal operations – in order to (i) support our key public service objectives, and (ii) maintain effective working relationships with our suppliers and dependants.

Key Deliverables

A Strategic Focus

- 9.1** Institute a strategic business planning focus within the office

Efficient Administration

- 9.2** To maximise the efficiency of the general administrative functions of the office

Good Financial Management

- 9.3** To manage the financial transactions of the office in a timely, efficient manner

Meeting Our Commitments

- 9.4** Ensure that Prompt Payments Act is adhered to as far as possible

Information Management

- 9.5** To effect an overhaul of the manual and electronic filing system to reflect good practice

New Accommodation

- 9.6** Manage the transition to new office accommodation

Objective 10:

To develop our ability to contribute in an effective way to international cooperation and to our international functions.

The Office is no longer limited in its functions to Ireland alone; we are also an integral element of the Data Protection infrastructure at European level. It is our objective to play a leading, formative role in our European operations and to be recognised internationally as an authoritative contributor.

Key Deliverables

The National Dimension

- 10.1** To establish national “first and third pillar” supervisory bodies

The Third Pillar

- 10.2** To strengthen our contribution to the Joint Supervisory Bodies

Article 29 Group

- 10.3** To strengthen our contribution to the Article 29 Group

International Relations

- 10.4** To enhance our good relations with other international data protection authorities

Transfers abroad

- 10.5** To supervise the transfer of personal data to third countries

Appendix 5

Receipts and Payments in the year ended 31 December, 2002

2001		2002
€	Receipts	€
524,874	Moneys provided by the Oireachtas (Note 1)	750,173
341,758	Fees	350,066
866,632		1,100,239
	Payments	
362,914	Salaries & Allowances (Note 2)	547,239
25,214	Travel & Subsistence	35,078
8,784	Office & Computer Equipment	10,275
1,665	Furniture & Fittings	646
12,178	Equipment Maintenance & Office Supplies	13,404
26,348	Accommodation Costs (Note 3)	11,491
10,765	Communication Costs	19,632
22,236	Incidental & Miscellaneous	44,448
54,770	Education & Awareness	58,912
	Legal & Professional Fees	9,048
524,874		750,173
	Payment of fees and legal refund receipts to Vote for the Office of the Minister for Justice, Equality & Law Reform	
341,758		350,066
866,632		1,100,239

Notes

- 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. The expenditure figures in this financial statement detail the payments made by the Department of Justice, Equality and Law Reform on behalf of the Office.
- Salaries, allowances and superannuation**
 - 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.
 - 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.
- Premises**
The Office of Public Works provides the premises at the Irish Life Centre, Talbot Street, Dublin 1, to the Commissioner without charge. The cost met by the Office of Public Works for this accommodation provided in 2002 was €65,000. (€63,835 in 2001)

Appendix 6

REGISTRATIONS 2000 / 2001/2002

(a) public authorities and other bodies and persons referred to in the Third Schedule of the Act

	2000	2001	2002
Civil service Departments/Offices	94	113	116
Local Authorities & VECs	111	118	139
Health Boards/Public Hospitals	55	56	57
Commercial State Sponsored Bodies	65	53	43
Non-Commercial & Regulatory	141	139	164
Third level	42	40	45
Sub-total	508	519	564

(b) financial institutions, insurance & assurance organisations, persons whose business consists wholly or mainly in direct marketing, providing credit references or collecting debts.

Associated Banks	38	35	42
Non-associated banks	60	60	58
Building societies	7	6	6
Insurance & related services	168	164	182
Credit Union & Friendly Societies	448	442	447
Credit Reference/Debt Collection	22	22	22
Direct Marketing	56	57	64
Sub-total	799	786	821

(c) any other data controller who keeps sensitive personal data

Primary & secondary schools	26	26	33
Miscellaneous commercial	65	53	79
Private hospitals/health	99	99	107
Doctors, dentists, health professionals	386	425	467
Pharmacists	491	643	667
Political parties & public representatives	96	90	95
Religious, voluntary & cultural organisations	51	57	91
Legal Profession	3	4	93
Sub-total	1,217	1,398	1,632

(d) data processors

	356	390	412
--	-----	-----	-----

(e) those required under S.I. 2/2001

Telecommunications/Internet	0	7	3
-----------------------------	---	---	---

TOTAL

	2,880	3,099	3,632
--	-------	-------	-------

