



Data Protection Commissioner

An Coimisinéir Cosanta Sonraí

Thirteenth Annual Report of the Data Protection Commissioner

2001

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

PN. 11693

Contents

Foreword	3
Réamhrá	5
Part 1 - Activities in 2001	
Introduction	8
Promoting Public Awareness	8
Enquiries	10
Complaints	11
The Public Register	12
Legislative Development	14
International Activities	15
Administration	19
Part 2 - Case Studies	
Cross Marketing of a Credit Card	22
Charity and Financial Institute Direct Marketing	24
Security of Employee Evaluation Data	26
Reusage of Credit Card Data	28
Teleappending and Direct Marketing	30
Uncooperative Legal Firm	31
Airline Booking and Passenger Data	33
Victim Support	34
Legal Firm Registration	35
Part 3 - Guidance Notes	
Codes of Practice	38
Considerations for the Health Sector	41
Appendices	
Appendix One - Receipts and Payments in 2001	45
Appendix Two - Registrations by Sector, 2000-2001	46
Appendix Three - Whats New in the Data Protection (Amendment) Bill?	47

Foreword

I am pleased to present this thirteenth Annual Report in relation to the work of the Office of the Data Protection Commissioner since it was established in 1989. It outlines in detail the activities of my Office during 2001.



Joe Meade
Data Protection Commissioner

When I presented my first report as Commissioner in early September 2001, I could never have imagined that a few days later the tragic and horrific attacks of September 11th would happen. This appalling attack on democracy has, quite rightly, led all democratic states and institutions to look at their security and anti-terrorism preventive measures. While measures of this nature are necessary, nevertheless it is also important to have regard to the principles of proportionality and specificity as any counter measures introduced should be adequately balanced against the needs to protect the fundamental human rights to privacy and personal data protection.

Due in the main to the extra burdens placed on the Department of Justice, Equality and Law Reform and the Attorney General's Office after the September 11th attacks, the expected transposition of the 1995 EU Data Protection Directive into Irish law did not materialise during 2001. This is regrettable as Ireland is now one of three EU countries who have not transposed its provisions. However I am pleased that the Minister,

- by order made in December 2001, brought provisions in the Directive regarding transfers to non-EEA countries and security measures into effect from April 2002
- initiated the Data Protection (Amendment) Bill, 2002, in February 2002, which, when enacted, will give effect to the other provisions of the Directive.

I accordingly look forward to the Directive being fully transposed during 2002.

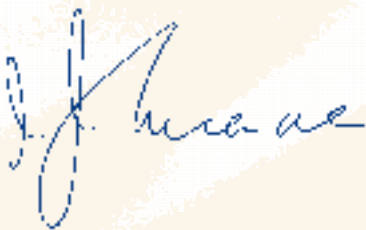
Previous Annual Reports have referred to the completely inadequate staffing resources of the Office and the position did not improve significantly during 2001. However I am grateful that the Department, in July 2001, got approval for extra posts to be allocated to the Office which are now being assigned. Even when the full complement are in place the position will not improve immediately as training and familiarity with highly complex and nuanced

legislation will be necessary. However I will still endeavour to improve the level of service provision in the next year.

The Report indicates that the year was a very busy one for the Office with increased levels of activity in all areas. This can be expected to continue as people quite rightly are concerned about their privacy and want my Office to investigate matters which concern them. I welcome this as it is proof that data protection is valued by people and that actions are necessary on my part to remind data controllers as to their responsibilities. With current resources I have in general had to adopt a policy of self registration by data controllers and not to initiate prosecutions when any other breaches of data protection law occurred. It is my intention, when the extra resources are in place, to pursue a prosecution policy, if necessary.

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 overall 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 am indebted to my office staff for once again ensuring, in very difficult circumstances, that a valuable public service has been provided overall in a timely, fair and efficient manner.



Joe Meade
Data Protection Commissioner

31 May 2002

Réamhrá

Is mian liom a chur i láthair an triú 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 2001.



Seosamh ÓMidheach
Coimisinéir Cosanta Sonraí

Nuair a chuir mé mo chéad Tuarascáil mar Coimisinéir i láthair go luath i Mí Meán Fómhar 2001 ní fhéadfainn a shamhlú go dtarlódh cúpla lá ina dhiaidh sin na hionsaithe tubaisteacha agus uafásacha ar 11ú lá Meán Fómhair. Chuir na hionsaithe allta sin ar an ndaonfhlaithreas iachall, agus an ceart acu, ar na stáit agus na hinstiúid daonfhlaithreacha breathnú arís ar a modhanna slándálachta agus frith gníomhaíocha sceimhlitheoireachta.

Bíodh is go bhfuil modhanna den cineál seo riachtanach, tá sé tábhachtach freisin i dtaca le prionsabail na comhréireachta agus na sainiúlachta de, go mbeadh aon frith modhanna nua a chuirfear i bhfeidhm meáite go cothrom i leith na riachtanais na cearta daonna bunúsacha do phríobháideacht agus cosaint sonraí pearsanta a chaomhnú.

De bharr i gcoitinne na hualaigh oibre breise a thuit ar an Roinn Dlí agus Cirt, Comhionannais agus Athcóirithe Dlí agus ar Oifig an Ard-Aighne i ndiaidh ionsaithe an 11ú Lá Mheán Fómhair 2001, níor thárla an taistriú a bhíodh ag súil leis den Treoir Cosanta Sonraí 1995 den Aontas Eorpach mar chuid de Dhlí na hÉireann i rith na bliana 2001. Is trua go bhfuil Éire ar cheann de trí tíortha san Aontas Eorpach nach bhfuil na forálacha sin aistrithe mar chuid dá dhlí fós. Mar sin féin tá áthas orm go bhfuil an tAire

- tré ordú a deineadh i Mí na Nollag 2001 forálacha an Treoir i leith aistrithe go tíortha nach cuid den EEU iad agus modhanna slándálachta a thabhairt i bhfeidhm ó Mí Aibreán 2002.
- An Bille um Chosaint Sonraí (Leasú) 2002 a thionscnamh i mí Feabhra 2002 ionnas nuair a achtófar é go dtabharfaidh sé éifeacht do forálacha eile an Treoir.

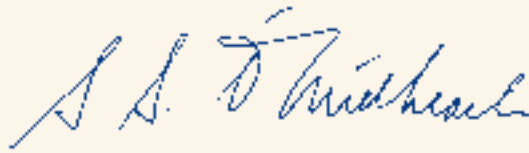
Táim ag súil, mar sin de, go naistreófar an Treoir ina dlí i rith na bliana 2002.

Deineadh tagairt i dTuarascáil Bliantúla cheana féin do easpa iomlán achmhainní foirne na h-Oifige seo agus níor tháinig aon fheabhas mórán ar an staid seo i rith na bliana 2001. Mar sin féin tá mé buíoch go bhfuair an Roinn i Mí Iúil 2001 cead postanna breise a dháileadh ar an Oifig agus tá siad á chur ar fáil anois. Fiú nuair a bheidh an líon iomlán ar fáil ní fheabhsóidh cúrsaí láithreach mar beidh gá le treineál agus taithi i leith reachtaíocht casta agus miondeifriúil. Mar sin féin, déanfaidh mé mo dhícheall an soláthar seirbhíse a fheabhsú i rith na bliana seo chugainn.

Léiríonn an Tuarascáil gur bliain an gnóthach ab ea an bliain seo don Oifig le leibhéal gníomhíochtaí breise i ngach réimse. Is féidir bheith ag súil leis seo mar go bhfuil daoine, agus an ceart acu, buartha mar gheall ar a phríobháideacht agus teastaíonn uatha go bhfiosródh mo Oifig nithe atá ag déanamh tinnis dóibh. Cuirim fáilte roimis seo mar is cruthú é gur luachmar le daoine cosaint sonraí agus go bhfuil gá le gníomhaíocht ó mo thaoibhse de a chur i gcuimhne do rialaitheoirí sonraí na dualgaisí atá orthu. Leis an achmhainn fóirne atá agam faoi láthair, do glacas i gcoitinne le polasaí féin clárú ag rialaitheoirí agus gan tús a chuir le hionchúiseamh nuair a tharla aon bhriseadh eile sa dlí ar chosaint sonraí. Tá rúin agam nuair atá an tacmhainn foirne breise ar fáil polasaí ionchúiseamh a leanúint más gá.

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 fhoirmhór rialaitheoirí sonraí a choimhlíon tríd is trí go hiomlán an dlí and 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 dhein 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 ÓMidheach

Coimisinéir Cosanta Sonraí

31 Bealtaine 2002



Part One
Activities in
2001

The Office of the Data Protection Commissioner is engaged in a diverse range of activities, both domestically and at international level. This section gives a comprehensive overview of the activities of my Office in 2001, with some emphasis upon a number of areas which I consider to be of particular interest.

Promoting Public Awareness

Data protection law is fundamentally an enabler, putting power into people's hands to protect their privacy rights. The first task of a Data Protection Commissioner, therefore, must be to educate the public both as regards the existence of data protection rights, and as regards the means of their enforcement. I have pursued these objectives in 2001 in the following principal ways:

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

Information booklets

Traditionally, my Office has published a range of information leaflets for distribution in response to queries from the public. In 2001, my Office distributed approximately 21,000 such leaflets. It is noticeable that the demand for this printed material has dropped significantly during the last year. I have no doubt that this is due in large part to the effectiveness of my Office's website (see below).

However, with imminent changes to data protection law, I anticipate that there will be a renewed demand for timely and comprehensive explanatory material across a range of media – printed, on-line and indeed broadcast.

I will also be considering new steps – such as independent market research – to evaluate the levels of public awareness about data protection and privacy issues, and to assess the impact of my various awareness initiatives.

Website information

I am delighted to report that the Office website – which went live in late 2000 – has proven popular and effective in 2001. Approximately 17,000 website hits were recorded in 2001, and the feedback from users – including members of the public and legal practitioners – has been very positive. I am also determined to invest resources in continually improving both the range and depth of public services on offer; to this end, I will take on board a number of useful and constructive suggestions I have received from website users. I would encourage the public to visit www.dataprivacy.ie to see for themselves the range of useful information, and indeed to offer further suggestions for improvement.

Media advertising

Expenditure on media advertising in 2001 totalled €39,300. As in previous years, advertising was targeted at a range of publications, in order to channel information both to the public in general, and to data controllers responsible for handling personal data. I indicated in last year's Report my intention to extend our advertising strategy to a wider range of media, including broadcast media. I anticipate that I will make good on this intention in the current year.

Direct contacts

Talks and presentations

While advertising and information of a general nature is a useful tool for improving overall levels of awareness, circumstances often arise where direct communication is essential – for example in addressing specific concerns or queries from particular groups. In 2001, my staff and I delivered presentations to a wide range of groups, of which the following are a representative sample:

- a) **Garda Training College, Templemore**
Myself and an assistant commissioner visited the Garda Training College for a useful discussion on ways to promote data protection awareness among Garda trainees, and among the force generally.
- b) **International Conference of Credit Reference Agencies**
This organisation held its annual meeting in Dublin in 2001, and I was glad of the opportunity to outline the approach adopted in Ireland to the issue of credit referencing and data protection.
- c) **Victim Support organisation**
I had a useful and productive exchange with this organisation – see case study 8/2001 (on page 34) for more details.
- d) **Financial Institutions**
I engaged in discussions with a number of major financial institutions which were anxious to ensure maximum compliance with data protection rules.
- e) **Motor industry**
My office made a presentation to representatives from the motor industry, regarding the application of data protection rules to forecourt-based IT systems
- f) **Irish Information Security Forum**
Given the key role that IT security systems play in underpinning data protection rights, my Office participated in this industry forum.

- g) **REACH**

The official body charged with implementing “e-Government” in Ireland is conscious of the need to respect data protection and privacy requirements, and towards this end I made a presentation to the body in 2001.

- h) **Department of Justice, Equality and Law Reform**

I made a presentation to the Department’s middle managers to impress upon them the importance of data protection law as a guiding principle of public policy.

- i) **Health Boards / Health Authorities**

Those charged with administering the healthcare system in Ireland must often confront issues of data protection, privacy and confidentiality, and my Office engaged in discussions with a number of authorities in 2001 to assist in addressing such issues in a practical way.

- j) **IBEC – Telecommunications sector**

I gave a presentation on data protection elements relating to telecommunications and internet services.

- k) **DIT – direct marketing course**

My Office contributed to those aspects of the DIT’s diploma programme relating to the legal regulation of direct marketing.

- l) **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, made good progress in its primary role of encouraging responsible self-regulation by the internet service industry, with a view to the prevention of illegal and harmful use of the internet. The Board also launched its website, www.iab.ie, which provides more information about its activities.

My Office continued to contribute to the work of the *Health Information Working Party*, an *ad hoc* group

Part One - Activities in 2001

convened by the Department of Health and Children to discuss standards for handling medical data in the health sector. As I made clear in last year's Annual Report, I believe that the handling of medical data within the health sector needs a major overhaul, to ensure that patient data can flow as medical treatment requires, while ensuring that medical confidentiality is accorded utmost priority. It is also important that medical practitioners at every level should have clear guidance on what is and what is not legally permissible. Towards this end, my Office's representatives on the Working Party have advocated the adoption of clear Codes of Practice for the health sector. I am optimistic that the Working Party's report, which is due shortly, will pave the way for significant progress in this area.

My Office also initiated discussions with the *Office of the Information Commissioner* so as to ensure that data protection law and Freedom of Information law – areas of law that are distinct in many ways, but which have close parallels in areas such as individual access to personal files – continue to operate smoothly. With the application in future of data protection law to manual files as well as computer files, it is important – for regulators, practitioners and the public alike – that there be clarity and useful guidance about the respective roles of the two sets of legislation. Useful discussions between our two Offices are ongoing.

Enquiries

The primary public service provided by my Office on a day-to-day basis is the provision of information and advice. Requests for such information come from individual members of the public, from organisations holding personal data ('data controllers'), and indeed from those involved in advising others (such as teachers, legal professionals, and citizens advice centres). I have devoted some resources to continued staff training so that the quality of advice offered can be as high as possible, and I am pleased to report that the feedback from those who contact my Office continues to be very positive.

It was my intention in launching a website in December 2000 that it would make a large amount of information on data protection easily available, thus reducing the time my staff would spend handling routine enquiries. It is certainly true that very many callers, on being advised of the existence of the website, are happy to pursue further information at their leisure from that source; this has certainly freed up staff time in handling routine matters. In addition, I have no doubt that many of the 17,000 visitors to the website are people who would otherwise have contacted my Office seeking information. This perhaps explains why the overall number of queries received in 2001, at 2,913, represents a small drop compared with the 2000 figure of 3,146. On the other hand, those queries that are received tend to be ever more complex in nature. This development is probably due in part to the technical nature of some legislative developments in the data protection area; and in part, perhaps, to the fact that callers are often better-informed as a result of having visited our website for preliminary information. In any event, the increasing sophistication of enquiries to my Office is, to my mind, a positive development, and an indication that awareness of the more basic data protection rules is now becoming more firmly embedded in the public mind.

As **figure 1** below shows, there have been slight increases in the numbers of enquiries received from data subjects and data controllers. Enquiries from other sources have dropped in comparison with 2000. Whilst the telephone is still the commonest method of contacting my Office, other methods are increasing in popularity. In particular, e-mail queries have risen sharply in number, and now account for 29% of enquiries received (See **figure 2** below.)

As regards the subject matter of the queries received, enquiries concerning access requests, checking a credit record and direct marketing remain the most common. Other subjects raised – most commonly by data controllers or their advisors – include the implementation of the European Data Protection Directive, the transfer of personal data overseas and the rules concerning the disclosure of data to third parties.

Part One - **Activities in 2001**

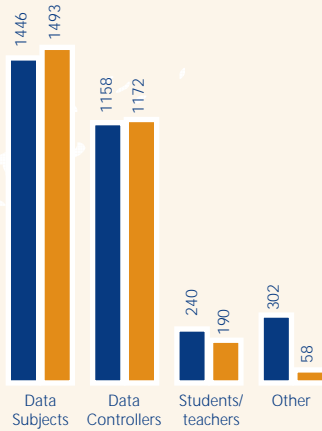


Figure 1
Contacts, sorted by category

● 2000 ● 2001

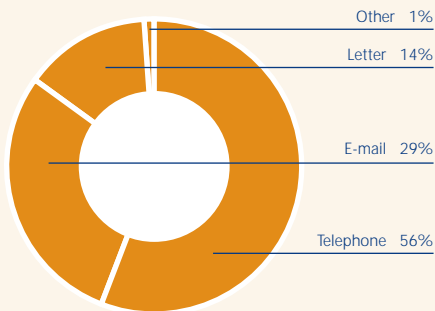


Figure 2
Contacts, sorted by contact method

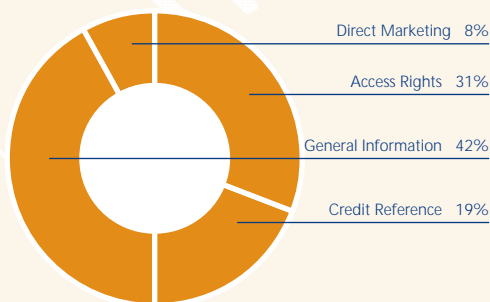


Figure 3
Data subject queries, sorted by topic

Complaints

The core function of my Office is the investigation of complaints raised with me by members of the public, in accordance with section 10 of the *Data Protection Act, 1988*. Individuals are entitled to complain to me if they consider that their data protection rights have been infringed in any way. 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.

The additional staffing resources (see under Administration below), which started to be allocated to my Office during the latter part of 2001, have had a marked positive effect on the complaints handling process. As the other staff promised to this Office arrive, and are trained to become effective members of my staff, I expect to be in a better position to finalise complaints effectively and speedily.

In 2001, the number of complaints processed formally rose to 233, a significant increase over the 2000 figure of 131. I should point out that the statistic is inflated somewhat by the relatively large number of formal complaints – 60 in total – in respect of issues with two particular data controllers. Even accounting for that factor, the throughput of complaints in my Office reached its highest level to date in the year 2001. **Figure 4** illustrates the level of complaints received, and the rate of processing them, in the past three years. While the figure for “complaints not concluded” has risen in both 2000 and 2001, I am confident that the allocation of much-needed staff resources will allow significant inroads to be made into the future. Indeed, the increase in the “complaints concluded” category is an indication that some progress is already underway.

Figure 5 shows a breakdown of the types of organisation against which complaints were made to this Office in 2001. One-third of complaints concerned central and local government, and financial services and telecommunications / IT sectors also accounted for a significant proportion of complaints. As regards the grounds for complaint –

Part One - **Activities in 2001**

see table 6 – the largest single bloc of cases involved concerns about the issue of fairness. This issue invariably involves 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. I would reiterate a point that has been made consistently through the years: 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. Other complaints involved disclosure of personal data to third parties, and difficulties in exercising the right of access to personal data. Of the complaints concluded I found that 35 % were upheld, 33% were not justified while 32% were resolved informally.

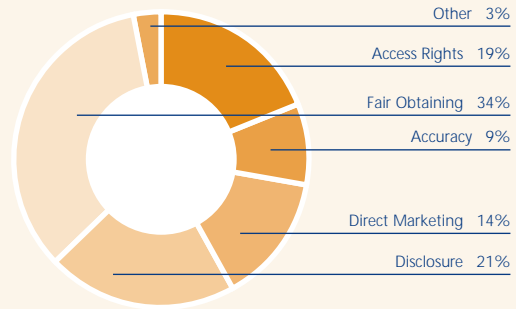


Figure 6
Breakdown of Complaints by Data Protection Issue

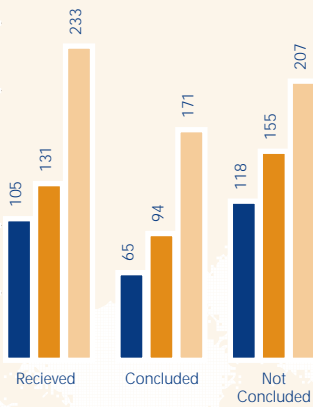


Figure 4
Complaints received, concluded and not concluded

● 1999 ● 2000 ● 2001

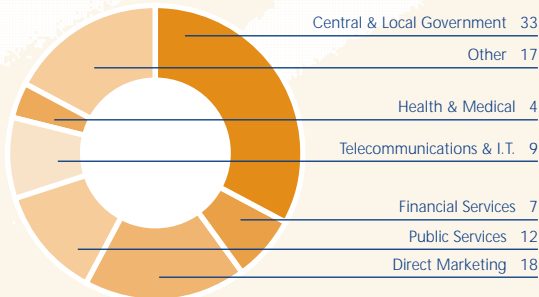


Figure 5
Breakdown of Data Controllers by business sector

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, which is available for inspection by the public, gives an indication of the types of personal data being kept by organisations, and the purposes for which the data are used. The number of registered persons had risen to 3,099 at the end of 2001, compared with 2,880 at the end of 2000 – an increase of 8%. 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 Two.

Part One - **Activities in 2001**

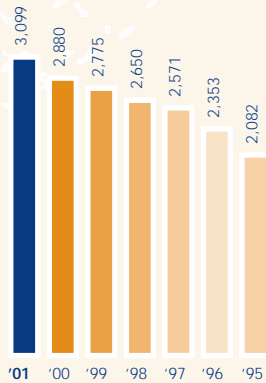


Figure 7
Number of Registrations

Registration of Telecommunications and Internet companies

A major initiative which I undertook in 2001 was the introduction of *Data Protection (Registration) Regulations, 2001*, which introduced a registration requirement for organisations providing internet and telecommunications services to individuals. This is the first time that the Data Protection Commissioner's power under section 16 of the Act to specify additional categories of registrable person has ever been exercised. I took this step in response to the important and growing role of internet and telecommunications services in people's lives, and in recognition of the need for public reassurances about privacy and data protection in this context. 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.

Progress in accepting registrations from the internet companies and telecommunications companies has been slow, in part due to the need for a fundamental re-assessment of data collection and retention policies. Discussions are ongoing and I expect to have applications finalized, on an acceptable basis, in the near future.

Registration and the Data Protection (Amendment) Bill, 2002

On another front, my Office is preparing for the changes likely following enactment of the *Data Protection (Amendment) Bill, 2002*. The Bill – which is of course subject to consideration and amendment by the Oireachtas – envisages a shift from the existing selective system of registration to a more comprehensive, 'universal' approach, as required by the terms of the European Data Protection Directive. However, the Bill envisages that I may issue regulations exempting certain categories of organisation from the registration requirement. I intend to exercise this power contemporaneously with the introduction of the new legislation, to ensure that the compliance burden is limited as far as possible to those data controllers whose operations might have some significant bearing upon individuals' privacy rights. I intend to liaise with practitioners and representative bodies on my specific proposals in this area.

Registration by the Legal Profession

In reviewing the entries in the public register, after my appointment to the position of Data Protection Commissioner, I noted that the number of legal professionals registered with my Office is very small indeed - 4 during 2001. I think it is to be expected, in the modern legal environment, that many legal professionals will have extensive day-to-day involvement with matters of a sensitive nature relating to the health, criminal convictions and ethnic background of their clients; and, indeed, that such matters will be recorded and processed on computer to some degree. Given that the keeping of such sensitive personal data on computer entails an obligation to register with my Office, under the terms of **section 16(1)(c)** of the *Data Protection Act, 1988*, I found it difficult to understand why the levels of registration from the legal profession have been so low.

I recognised that levels of awareness among the legal profession regarding the registration provisions of the Act might not be as high as they should, and

Part One - Activities in 2001

accordingly, before I considered the possible recourse to the legal enforcement powers open to me, I made contact with both the Law Society and the Bar Council in 2001.

The Law Society indicated that it was a matter for each individual member to decide whether a registration requirement arose or not but it agreed to include a reminder in its Law Gazette. This reminder appears to have elicited no positive response from any solicitors.

Likewise, the Bar Council's initial response was that registration was a matter for individual members to determine. The Bar Council pointed out that some barristers would have little, if any, requirement to retain sensitive computer files; although it was accepted that, in practice, many barristers would inevitably retain files on their computer hard-drives that included reference to 'sensitive' details such as criminal convictions, personal injuries, ethnic origin and so on. The Bar Council has recently informed me of its intention to bring the data protection registration requirement to the notice of its members by issuing a circular on the matter. I think it is fair to acknowledge the Council's seriousness of purpose in this regard.

Notwithstanding this welcome initiative from the Bar Council and the earlier Law Society's reminder, I remain concerned that legal professionals – a great many of whom must surely, in this day and age, be keeping personal data of a sensitive nature on computers which they control – have failed to register with my Office, in contravention of the provisions of section 16 and 19 of the Data Protection Act. Indeed, section 19(6) of the Act provides that failure to register is an offence.

While I regard this as a serious matter, I have to date, due to resource constraints, had to rely to an extent on 'self registration' by data controllers. With increased resources coming to my Office I plan to review this area in greater detail than was possible up to now.

Legislative Developments

Those with an interest in or an awareness of data protection matters will know that the implementation in Irish law of the 1995 European Data Protection Directive, 95/46/EC, is now long overdue. 2001 saw the first moves towards implementation, with the introduction in December 2001 by the Minister for Justice, Equality and Law Reform of the *European Communities (Data Protection) Regulations, 2001*. The Regulations implement (with effect from 1 April 2002) some of the provisions of the Directive, principally those dealing with transfers of personal data to "third countries", i.e. countries outside of the European Economic Area (EEA). An explanatory guide to the Regulations is available on my Office website, www.dataprivacy.ie.

More recently, the publication in February 2002 of the *Data Protection (Amendment) Bill, 2002* represents a major step towards the implementation of the Directive in Ireland. The Bill, which is subject to consideration by the Oireachtas, deals with all of the Directive's requirements, as well as addressing some additional matters. Again, guidance material on the contents of the Bill is available on my website.

The other main EU instrument in the area of data protection is Directive 97/66/EC, dealing with data protection in the telecommunications sector. I am pleased to note that this Directive has recently been transposed into Irish law by the Minister for Public Enterprise via the *European Communities (Data Protection and Privacy in Telecommunications) Regulations, 2002*.

International Activities

It is my firm view that national data protection authorities can no longer address privacy issues in isolation from our colleagues – not just within Europe, but around the world. This is so because of the transnational reach of global commerce, the realities of today's internet and e-commerce environment – and also, importantly, because of the universal interest in promoting and protecting the fundamental human right to privacy. The range of international activities of my Office is detailed below.

Article 29 Working Party

The Article 29 Working Party is a consultative body made up of Data Protection Commissioners from the EU Member States together with a representative of the EU Commission. The Working Party met regularly during 2001 and my Office participated in all of these meetings. The following were the main matters of interest discussed during the year.

Processing personal data in the employment context

Much debate took place on this important subject before an opinion was adopted in September 2001. My office was represented on a sub-group which considered the matter in detail. The group based its work on the principle that the collection, use, or storage of information about workers, the monitoring of their email or internet access or their surveillance by video cameras (which process images) involves the processing of personal data and, as such, data protection law applies to such processing. However, data protection law and employment law do not operate in isolation from each other. Interaction is necessary and valuable and should assist the development of solutions that properly protect workers' interests. Furthermore many Member States have different legal requirements regarding labour law and privacy in the employment context. Taking these factors into account the Working Party opined *inter alia* that:

- the legitimate interests of the employer (to lawfully process personal data that are necessary for the normal development of the employment relationship and the business operation) justify certain limitations to the privacy of individuals at the workplace. Sometimes it is the law or the interests of others which impose these limitations. However, no business interest may ever prevail on the principles of transparency, lawful processing, legitimisation, proportionality, necessity and others contained in data protection laws. A worker can always object to the processing when it is susceptible of unjustifiably overriding his/her fundamental rights and freedoms
- many activities performed routinely in the workplace entail the processing of personal data of workers
- monitoring of emails necessarily involves the processing of personal data
- processing of sound and image data in the employment context falls within the scope of the Data Protection Directive
- monitoring and surveillance whether in terms of email use, Internet use, video cameras or location data are subject to data protection requirements. Any monitoring must be a proportionate response by an employer to the risk it faces taking into account the legitimate privacy and other interests of workers. Any monitoring must be carried out in the least intrusive way possible
- monitoring, including surveillance by camera, must comply with the transparency requirements of data protection law. Staff must be informed of the existence of the surveillance and the purposes for which personal data are to be processed
- at a very minimum staff need to know what the employer is collecting on them (directly or from other sources). Staff have a right of access to their data under section 4 of the Data Protection Act, 1988
- the personal data should be relevant, adequate and not excessive in relation to the purpose for which it is collected and processed

Part One - Activities in 2001

- staff in charge of or with responsibility for the processing of personal data of other workers need to be aware of data protection and be adequately trained
- where processing is necessary as a result of the employment relationship, it is misleading to seek to legitimise this processing through consent. Reliance on consent should be confined to cases where the worker has a genuine free choice and is subsequently able to withdraw the consent without detriment
- robust security systems should be in place to prevent unauthorized access to personal data.

Because monitoring of private emails and private use of the Internet in the workplace pose certain challenges the Working Party is developing a position paper during 2002 which will aim to provide guidance on the minimum content of employers' policies in this area.

Post September 11 situation

The Working Party recognized that the horrific attacks of September 11, 2001 have inevitably led democratic governments to consider their anti-terrorism procedures and to initiate new measures in this area. It is important, however, that such initiatives should not displace peoples' fundamental right to privacy, and accordingly any such measures need to be of a balanced and proportionate nature. The Working Party for its part has emphasised that privacy and data protection should in no way be seen as a barrier to efficient fight against terrorism. Indeed, I would contend that the opposite is rather the case: privacy is one of the fundamental values that form the basis of democratic societies – the very values and the very societies that terrorists seek to destroy – and accordingly such values should be prized and preserved all the more vigorously, even in such trying times.

Model contracts for data processors

A new standard or 'model' contract was approved by the Commission, after consultation with the Working Party, to facilitate the international transfer of personal data to data processors established in 'third countries'. Following consideration of drafts the Working Party outlined its overall approval of the Commission's proposals in September 2001. The Commission approved the matter in December 2001 and the provisions came into effect from 1 April 2002. This model contract is in addition to the model contracts already in existence for data controllers who transfer personal data to other data controllers in third countries. Copies of the contracts can be downloaded from the Commission website.

Approval of third countries

Another function of the EU Commission is to consider the adequacy of data protection legislation in place in 'third countries'. By 2000, the EU Commission confirmed that the systems in place in Hungary and Switzerland were adequate and during 2001 aspects of Canada's system were also considered adequate, on foot of recommendations to this effect from the Working Party. Other countries' systems are the subject of ongoing review.

Minimum requirements for collecting data online

The Working Party issued an important Recommendation regarding data protection in the context of on-line transactions. In essence, adequate means should be in place to guarantee that Internet users get all the information they need to place their trust, in full knowledge of the facts, in the sites with which they enter into contact; and if need be, to exercise certain choices in accordance with their rights under data protection law. The recommendation of the Working Party outlined a minimum set of concrete measures to be put in place – openness and transparency regarding their collecting processes and their security features – while alerting individuals to what they should expect before they supply data on line.

Part One - Activities in 2001

In effect, at initial contact between an Internet user and a web site, the person should know how his/her data is protected, whether the contact is for the purpose of seeking information or to conclude a commercial transaction on a step-by-step basis. The web-site should state the identity and physical and electronic address of the controller; the purposes of the processing; whether information to be provided is obligatory or optional; the manner in which the right to consent or to object to processing of personal data may be exercised; the manner in which the right to access, rectification and erasure of data may be exercised; whether data will be disclosed to third parties and if so there should be the facility to object on-line. A clear privacy statement in simple language would enhance matters in this regard and this statement should be able to satisfy a privacy audit if it was carried out by a data protection authority. Certain standards relating to the use of 'cookies' are also addressed in the recommendation.

Applicant countries

The Working Party agreed to the attendance at its meetings of independent data protection bodies in those countries who have applied to join the EU. These bodies attend as observers but can contribute to various matters being discussed. This ensures that when the applicant countries join the EU they will be well aware of how the Working Party works while it is enriched by their contributions at present. In this way a better understanding of problems is attained.

The Working Party also considered the implications of the Cybercrime convention as well as many general data protection issues.

The detailed recommendations of the Working Party are available on the Commission's web site, which is accessible via the links section on my website, www.dataprivacy.ie.

Supervision of Europol

My Office continued to play a full role in the Europol Joint Supervisory Body (JSB), which meets in Brussels on a quarterly basis to supervise the operation of Europol, the European Police Office. The implementation of a dedicated secretariat to service the JSB and other "third pillar" bodies (see below) helped to improve the efficiency and effectiveness of operations. The activities of the JSB during the period 1998-2001 will be detailed in an activity report, to be published in the near future. Any such material will be accessible via my Office's website, www.dataprivacy.ie.

Domestic supervision

The allocation of some additional staffing resources to my Office during 2001 will enable my Office to initiate the functions assigned to me under the 1997 Europol Act, in acting as the national supervisory body for the Europol "national unit". This is a unit of An Garda Síochána responsible for liaising with Europol headquarters in The Hague, the Netherlands.

Other Third Pillar" Initiatives

The "third pillar" of the EU refers to items in the area of police and judicial cooperation in criminal matters, including cooperation by customs authorities in this area. The establishment of Europol is one measure in this area; another initiative is the Customs Information System (CIS), which allows for EU-wide cooperation in dealing with customs matters. In fact, there are two major elements to customs cooperation within the EU: the first element concerns traditional customs payment and administration matters, and is dealt with under the "first pillar", or conventional Community system of the EU; the second element, concerning cooperation in customs-related criminal matters, is dealt with under the "third pillar" procedures. My Office has a role to play in the data protection supervision of both elements. As regards the third pillar side, a Joint Supervisory Body for the Customs area was initiated in 2001, with full

Part One - Activities in 2001

participation from my Office, and its substantive work is now under way.

A related but distinct matter is the Schengen Agreement. The objective of this Agreement, which is founded upon the 1990 Schengen Convention, is to secure border-free travel within participating EU Member States (as well as Norway and Iceland); the arrangement also requires a database (known as the Schengen Information System or SIS) to address the security and immigration concerns of participating States. An EU Decision has only recently been made concerning Ireland's application to accede to some parts of the Agreement, and so my Office had no formal role in 2001 in the data protection supervisory body – known as the Schengen Joint Supervisory Authority (JSA) – that supervises the SIS database. However, my Office now has official observer status on the JSA, and is involved in discussions under the auspices of the Department of Justice, Equality & Law Reform with a view to implementing the necessary arrangements at national level.

No substantive progress was made at EU level in 2001 on the proposed 'Eurodac' system, which is intended to facilitate Member States in exchanging fingerprint data about asylum applicants; and consequently my Office had no involvement in the data protection elements of this matter in 2001.

International Conferences

The 23rd annual International Conference of Privacy and Data Protection Commissioners was held in Paris in September 2001, and my Office was represented. The Conference is an open forum for data protection authorities from around the world, and other interested parties, to discuss and debate developments of common interest. The 2001 Conference included important discussions on items including: biometrics and facial recognition technologies; localisation techniques; technology for privacy protection; and the interplay of data protection and measures to combat cybercrime. I am pleased that the United Kingdom and Irish data protection authorities, together with the authorities of Guernsey, Jersey and the Isle of Man, will jointly be

hosting the 24th International Conference, to take place in Cardiff in September 2002. This initiative is very much in keeping with the warm spirit of co-operation that exists among our island colleagues.

The annual Spring Conference of European Data Protection Commissioners is an opportunity for Europe's data protection authorities to exchange their knowledge and experience. In May 2001 the conference took place in Athens and my Office participated. Discussion focused on a number of issues including: cybercrime, retention of telecommunications data, protection of workers' data, e-commerce, and the issue of 'blacklists' for consumer credit.

International Complaints Handling Workshops

As I outlined in last year's Annual Report, the twice-yearly international workshops to discuss approaches to complaints-handling have proven to be informative and effective. In 2001, workshops were held in Oslo and Lisbon and were attended by staff from my Office. The web-based forum, established to facilitate and build upon the workshop, has also proven most useful as a tool of international cooperation.

Council of Europe Conference

The Polish authority in association with the Council of Europe organized a conference in Warsaw in November 2001. The conference dealt mainly with international cooperation among data protection authorities, in the light of a new protocol to 'Convention 108' – the Council's 1981 data protection convention. I had the honour to be asked to address the conference to outline Ireland's situation. More and more international authorities realize that such cooperation is vital in an ever-expanding global environment if personal privacy is to be enhanced.

Part One - **Activities in 2001**

British and Irish Data Protection Authorities

The British and Irish data protection authorities (including those from the Isle of Man, Guernsey and Jersey) continued our series of twice-yearly roundtables in 2001, with useful meetings in Guernsey and Manchester.

Equality and Law Reform in this regard, and to acknowledge their commitment to allocating the further staffing and other resources necessary to enable my Office to fulfil its mandate.

Administration

Running Costs

The costs of running the Office in 2001 are as set out in Table 1 below. Figures for 2000 are given for comparison.

Table 1 Costs of running the office in 2001

	2000 €	2001 €	% change
Overall running costs	500,951	588,709	18%
Receipts	311,344	341,872	10%
Receipts as % of running costs		62%	58%

A fuller account of receipts and expenditure in 2001 is provided for information purposes in Appendix 1.

Staffing

In last year's Annual Report, I set out in some detail my concerns regarding the inadequacy of my Office's level of staffing, having regard to the increasing – and increasingly complex – requirements of data protection law and its enforcement. I am very pleased to note that the staffing complement has now begun to be addressed in a meaningful way. The staffing level, which stood at seven at the time of last year's Report, has now doubled to fourteen. While there has been some delay in getting the full approved complement in place, I am happy to acknowledge the positive response of the Department of Justice,

Support Services

The technological environment within the Office has been continually upgraded during 2001, a process that has been facilitated to a significant degree by the IT Section of the Department of Justice, Equality and Law Reform. 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 an invaluable service in the area of receipts and payments.





Part Two

Case Studies

Case Study 1

Bank and insurance company – cross-marketing of a third-party product – incompatible use and disclosure – fair obtaining and processing – small print and transparency

The complainant received a letter from his insurance company, informing him of their new credit card, and enclosing an explanatory booklet and application form. The complainant duly completed and returned the application form. Subsequently, he was contacted by a bank in connection with his credit card application. The bank – with which the individual already had a credit card account – queried the level of credit being sought by the individual, in the light of his existing credit card account.

The individual was most unhappy that the insurance company had apparently transferred his confidential personal data to another financial institution without his consent. The insurance company explained that they had an agreement with the bank, which was the issuer of the credit card, and that there was therefore no basis for his complaint.

The individual complained to my Office and made the following points:

- The correspondence he had received from the insurance company enclosed an explanatory booklet and application form which referred throughout to the credit card as the insurance company's card. It also enclosed a return envelope addressed to the insurance company.
- He clearly was given to understand that the communication from his insurance company was an offer to him to do further business with that company. The personal data which the company had used to contact him, and the information which he had furnished in his application, was of a confidential nature, and was to his mind a

...any 'cross-marketing' exercise of this or similar nature should, in future, clearly indicate - with suitable prominence - the real identity of the companies involved...

matter of private business between himself and his insurance company.

- He did not want this confidential information to be disclosed to anyone other than the insurance company. In particular, he did not want the bank to have access to this information, and it was now apparent that the bank was seeking to use these confidential details to vary his existing credit limits.

In Data Protection terms, the essence of the complaint was that the insurance company had used and disclosed the complainant's personal data in a manner incompatible with the purpose for which the data had been obtained (contrary to section 2(1)(c)(ii) of the Data Protection Act); and that the bank had obtained and processed the complainant's data unfairly, contrary to section 2(1)(a) of the Act.

In investigating the 'fair obtaining' aspects of this complaint, I considered it appropriate to examine in detail the documentation that accompanied the credit card offer, I noted that on the front of the application form applicants were advised to send the completed application form, in a provided "freepost" envelope, to what appeared to be the insurance company's address. In fact, my investigations established that the address was really that of the bank. The promotional literature and application form clearly marketed the credit card as an offering of the insurance company. References to the 'insurance company credit card' were in large, colourful print and were given considerable prominence. I noted that the only references to the bank, as issuer of the credit card, were contained in the 'small print' of the application form, setting out the detailed terms and conditions. Indeed, the brochure appeared to distinguish 'its'

Part Two - Case Studies

credit card from those offered by other financial institutions, including the bank in question: the brochure listed, for comparison, the interest rates payable on credit cards of nine other financial institutions, including that particular bank.

On raising the complaint with the insurance company and the bank, it was explained that a formal agreement was in place whereby the bank was the issuer of the credit card, and the insurance company acted as agents for marketing the card – a practice referred to in this context as ‘cross-marketing.’ On receipt by the bank of the complainant’s application form, his personal details were inputted onto the bank’s computer system, and a routine check was made against the bank’s database for any cards currently held by the applicant. This check highlighted the existence of the complainant’s existing credit card with the Bank.

After detailed consideration of the matter, I reached the following conclusions:

- It was clear from the nature of the Agreement between the insurance company and the bank that the bank was envisaged as being the data controller in respect of the credit card which was on offer; and as such the bank was responsible for ensuring that the obligations imposed on data controllers by section 2 of the Act were complied with. In all of the circumstances of this case, the necessary prerequisites for ‘fair obtaining’ had not been met by the bank.
- The insurance company kept personal data relating to the complainant for purpose of administering his insurance policy, and for related secondary purposes. In inviting its customers to apply for the credit card, the insurance company had used their own customer database for a different and unrelated purpose, namely the direct marketing of a third-party product – the bank’s credit card. The insurance company did not produce any evidence that the unrelated purpose was supported by the necessary consent. Accordingly, the insurance company was in contravention of section 2(1)(c)(ii) of the Act, which prohibits the use or disclosure of personal data in a manner incompatible with the specified purpose.

In coming to this decision, I noted that the insurance company had undertaken to revise the documentation to give appropriate prominence to the role of the bank. I also noted the view of both organisations that they had acted in good faith throughout, pursuant to the Agreement between them.

Finally, I pointed out to both parties – and drew to the attention of the Central Bank – that, as regards data protection law, any ‘cross-marketing’ exercise of this or similar nature should, in future, clearly indicate – with suitable prominence – the real identity of the companies involved, in a manner readily apparent to any reasonable person. This case also brought to light an interesting interplay between data protection law and the general law of contract. While contractual agreements may be legally valid (having regard solely to the provisions of general contract law), this does not obviate the need to comply with data protection rules – including the fair obtaining rule – when processing personal data in pursuance of a possible contract. Whether, and to what extent, the contractual validity of an agreement may be affected by a deficiency in terms of data protection law – such as a failure in regard to fair obtaining – is a question on which the courts may eventually be called upon to adjudicate.

Case Study 2

Major charitable organisation – disclosure of donors’ details to a financial institution – pro-active investigation – unfair obtaining – consent

Members of the public alerted a national “phone-in” radio show to the fact that they had been receiving mailings from a financial institution, which appeared to be aware that the individuals had made donations to Concern, a respected national charitable organisation. A representative of Concern explained on the radio show that the organisation had allowed the financial institution to promote its products by mailing Concern donors, without the express consent of these individuals. In return for offering this facility, Concern received a payment for each individual who responded positively to the direct mailing. The Concern representative indicated his belief that this practice was permissible under the Data Protection Act.

Having heard this interview, I immediately contacted Concern to request an urgent meeting and the meeting took place that same day. At this meeting, I pointed out that personal data held by Concern in relation to its donors should not be used or disclosed in a manner incompatible with the purpose for which the individuals had provided their details. I asked Concern to outline the method used to collect data. The Concern representatives produced a printout from the Concern web site, showing the sort of data requested from subscribers and the ‘opt-out’ boxes used on the form. These ‘opt-outs’ asked (a) if a person wanted to receive any further marketing, or (b) if the person consented to data being shared with “like-minded organisations”. The same questions were asked in postal or telephone variants.

As regard the direct mailing campaign, Concern informed me that they had been approached by a marketing company which had suggested an ‘affinity arrangement’ with the financial institution in

...There is no data protection objection to affinity relationships in principle, as long as such relationships are carried out in a proper and transparent manner, including appropriate clear and informed consent...

question. In essence, Concern would make its list of donors available to the direct marketing company, which would issue special promotional mailings to the individuals on the list. Whenever any individual responded positively to the promotional offer, the financial institution would make a payment to Concern. This scheme appeared to offer advantages to all sides, and the agreement was made on this basis. A confidentiality agreement was put in place between Concern and the direct marketing company, so that no personal data would be disclosed to the financial institution itself.

Having considered the nature of the arrangement, I found that it was unsupported by the necessary levels of consent from Concern donors. I did not accept that a financial institution was a “like-minded organisation” of the sort envisaged in the Concern donation form. Accordingly, the use of the Concern database to facilitate direct marketing by financial institutions was not, to my mind, compatible with the purpose for which Concern had obtained the data, and therefore this was not a legitimate use of these data. **Concern fully accepted my viewpoint on this matter; indicated that the process was to cease immediately; and undertook to ensure compliance with the Data Protection Act in future.** Concern indicated – and I fully accepted – that they had never intended to be in breach of data protection law or to be in any way disrespectful of their donors’ privacy.

In no way do I, as Data Protection Commissioner, want to prevent the flow of much-needed money to any respectable charity such as Concern. There is no data protection objection to affinity relationships in principle, as long as such

Part Two - Case Studies

relationships are carried out in a proper and transparent manner, including appropriate clear and informed consent. While in this particular instance Concern inadvertently breached data protection law, the prompt manner in which the organisation responded to my unease assures me that Concern take their data protection responsibilities seriously.

Case Study 3

Employee performance ratings disclosed to other staff – inadequate security

I received a letter of complaint from a number of employees within a particular company. It appeared that the company had created a computer file setting out performance assessment reports for individual members of staff. The file – of which staff members had been unaware – was accessible throughout the company to a wide range of line managers, including managers who had no role in relation to the staff members in question. The employees were concerned that their data protection rights had been infringed by the unnecessarily widespread dissemination of confidential personnel details, and they asked me to investigate the matter.

On raising the issue with the company, it was explained that the line manager of a particular unit had created a file, setting out performance ratings for staff under his supervision. However, the “access permissions” on this file had inadvertently been set to allow numerous people outside of his management team to read it. A staff member who noticed this problem had brought it to the attention of management, and the file in question was destroyed. The company had also arranged for a formal investigation into the matter, which had concluded that there had been –

- a failure to adequately protect and secure sensitive information held on the staff within the particular business unit
- insufficient detailed knowledge by managers of the security environment in which the data were held
- a failure by the staff member who initially discovered the file to alert the appropriate manager to its existence, as required under various HQ policies and the unit's own confidentiality statement

...the failure to implement appropriate access restrictions contravened the security requirements of the Act ... and the resulting dissemination of the file to other unauthorised staff members amounted to an incompatible disclosure of the personal data ...

- subsequent failures by some staff members to prevent ongoing disclosure of the contents of the file.

The company accepted these findings and that a breach of the *Data Protection Act, 1988* had occurred in this incident. They acknowledged the need to address these issues, and had put in place the following measures –

- an immediate training programme in IT security for all managers and staff, together with regular refresher programmes
- all remaining hard- and soft-copies of the file in question to be destroyed as a matter of the utmost urgency, with all company systems swept to confirm this
- HQ policies on security should be reissued to all managers and staff
- standards for holding sensitive data, both personal and commercial, to be reviewed and published.

As regards my own findings, I accepted that, in an employment context, staff members may not automatically have the option of objecting to their data being used for appraisal purposes – this would naturally depend on conditions of employment and industrial relations norms. However, I concluded that staff should be made fully aware of new appraisal initiatives which involve the use of their personal

Part Two - Case Studies

data, if the 'fair obtaining' requirements of **section 2(1)(a)** of the Act were to be respected. The performance appraisal file in this case had not met these standards, and so its creation entailed a contravention of the Act.

I also confirmed that the failure to implement appropriate access restrictions contravened the security requirements of the Act (**section 2(1)(d)**), and that the resulting dissemination of the file to other unauthorised staff members amounted to an incompatible disclosure of the personal data (contrary to **section 2(1)(c)(ii)** of the Act).

However I was pleased to note that the Company had taken immediate and appropriate steps to address the issues involved in this case, particularly in terms of ensuring that appropriate security measures are in place and improving awareness of staff and management regarding the importance of adhering to correct procedures. I believe that this case is a useful reminder of the need for appropriate internal security measures – both as regards the pitfalls, and as regards the correct way to address any deficiencies that are identified. This issue now takes on an added importance with the implementation in Ireland, from 1 April 2002, of the revised security provisions introduced in the *European Communities (Data Protection) Regulations, 2001*, which have transposed certain provisions of the European Data Protection Directive into Irish law.

Case Study 4

Credit card transaction – use of details from a previous transaction without consent – fair obtaining – transparency – retention period

A customer of a car rental company alleged that the company had used his credit card data – obtained in a previous transaction – to process a disputed charge without his consent, and in spite of his objections to the charge.

The facts were that a motor car, purchased by the complainant, had given trouble and the garage had arranged a courtesy car with a car rental firm while his own car was being repaired. Prior to taking the car, he inspected it and agreed that it was not in any way damaged. One week after returning the car, the complainant was asked by the rental firm to sign a damage report on the car, and he was informed that he was liable for payment of a £250 charge. He denied all knowledge of damage to the rental car. The rental firm informed the complainant that they would collect the charge of £250 via his credit card. He maintained that he had not given his account details to the rental firm on this occasion, although he had in the past hired numerous vehicles from them which he had paid for by credit card.

The specific data protection issue in this case was whether the rental firm obtained and processed the complainant's credit card details fairly, with the appropriate level of consent from the individual.

When I raised the matter with the car rental firm, they maintained that the complainant was liable for the cost of repair of the vehicle under the terms of the agreement which he had signed. They also stated that the complainant's credit card details had been obtained and processed fairly; were kept for a specified and lawful purpose; and were not used in any manner incompatible with that purpose. Furthermore, the use of the credit card details in this

...credit card data obtained for a particular transaction cannot be used subsequently for other transactions without express consent, without violating the 'fair obtaining' rule...

instance was specifically for the purpose envisaged in the rental agreement.

I asked the firm to provide evidence of the circumstances in which the complainant had given them his credit card details. They replied that staff did not recall whether the complainant had provided his credit card details specifically for the purpose of the rental in question, or whether the complainant had consented to the use of his credit card details, which he provided on a previous occasion. However, they also stated that the clearing bank had confirmed that the complainant's credit card details had been manually keyed into the credit card machine when the car was being rented. On further investigation I found that there was no record of any credit card details on the copy of the rental agreement supplied for that date by the rental firm. Taken together, these facts strongly suggested to me that the rental firm's sales staff had used details provided and noted on a previous rental agreement. If it was standard practice to use the data previously obtained, as the firm claimed, this should have been made known to the data subject at the time of first obtaining the data, and consent obtained for this practice. It should also have been noted on the rental agreement in this instance that the customer had consented to the use of details provided on a previous occasion.

As regards the retention period of credit card details that had been obtained in the past, the rental firm argued that retention was necessary for audit and legal purposes. While I was prepared to accept this line of argument to a certain extent, I observed that – in general – details of a contract, which is no longer in dispute, should be deleted once the contractual relationship has ceased. In addition, there is no need

Part Two - Case Studies

to retain such data beyond the end of a particular audit period. Furthermore, in the interim – i.e. while the data are being retained for necessary legal or audit purposes – the data should not be used for any other purposes without the express consent of the data subject.

I was satisfied that in the present case, given the manner in which the credit card details were obtained, the data controller had failed to achieve transparency and informed consent and that the necessary prerequisites for fair obtaining had therefore not been met. Accordingly, I found that the rental firm had contravened the Act and I upheld the complaint against them. In response to my decision, the rental firm stated that, in order to avoid a recurrence of the situation leading to this dispute, they were ceasing the practice of using previously-obtained credit card details, and that customers would in future be required to provide their details whenever they entered into a new rental agreement.

This is an outcome which I welcome, and which is likely to avert similar data protection complaints in future.

More generally, I consider it to be a sound and proper principle that credit card data obtained for a particular transaction cannot be used subsequently for other transactions without express consent, without violating the 'fair obtaining' rule. The principle of transparency and fairness, which are key tenets of data protection law and practice, apply in this area just as in any other.



Case Study 5

MBNA Bank – unwanted direct marketing – mailings and telemarketing – failure to delete details from direct marketing databases – Eircom – the practice of ‘teleappending’ – fair processing – incompatible purpose

A number of individuals contacted my Office to complain about the receipt of direct marketing contacts from MBNA Bank, a financial institution specialising in credit cards. Some individuals were unhappy about receiving unsolicited telephone calls at their homes, while one individual – who had received a number of unwanted mailings and telephone calls over a period of several months – had gone to some lengths to remove his details from MBNA’s direct marketing databases, but apparently without success. In investigating this series of complaints, two distinct but related issues arose for consideration: (i) MBNA’s response to individuals’ requests to opt out of direct marketing, and (ii) Eircom’s practice of adding telephone directory details onto other large databases – the practice of ‘teleappending’. Both will be considered in turn.

As regards the difficulties and concerns of individuals with regard to direct marketing, I raised the issue with MBNA and found the bank to be cooperative and helpful. The bank stressed its desire to comply fully with data protection law, and I had no reason to doubt the bank’s bona fides in this regard. At a meeting with MBNA representatives, the bank explained that personal information was obtained from two principal sources: application forms (which included an ‘opt-out’ tick box, for those who did not wish to receive direct marketing), and a direct marketing agency called PMI, which maintains an extensive database (derived in large part from the electoral register) to facilitate direct marketing of Irish residents. The bank was fully aware of individuals’

...The bank was fully aware of individuals’ legal right to be removed from direct marketing databases...and acknowledged that its procedures had clearly failed for the complainant in this case...

legal right to be removed from direct marketing databases, and had detailed procedures in place to ensure that this right was honoured. The bank acknowledged that these procedures had clearly failed for the complainant in this case.

My office insisted that fuller details be provided as to why the procedure had failed so badly in the case of the particular complainant in question. Having investigated the matter, MBNA concluded that the problem had arisen due to deficiencies in communication with its direct marketing associate, PMI. MBNA said that more stringent checking procedures had been put in place, and that direct marketing staff had been re-educated, with a view to addressing these deficiencies.

Section 2(7) of the Data Protection Act, 1988 provides that, on request, a person’s name must be removed from a direct marketing list. In the circumstances of this case, I concluded that the Bank was, in this instance, in breach of its data protection obligations. **I also found it appropriate, in the interests of fairness, to place the Bank’s failure in this instance in proper context.** I noted that the Bank issues of the order of 2,000,000 direct mailings every year, and process about 40,000 “do not contact” requests. The evidence would appear to indicate that they succeed in complying with the great majority of such requests, and I had no basis for doubting their stated commitment to complying with data protection law. I also noted that the bank had taken concrete steps to prevent a recurrence of this matter.

Part Two - Case Studies

'Teleappending'

As regards the separate issue of telephoning people at home, MBNA explained that the phone numbers had been made available for direct marketing purposes via Eircom. I therefore decided it would be appropriate to raise this matter with that organisation, which was the data controller in respect of the telephone directory database. In my discussions with Eircom, I established that the phone company offered a commercial service to clients, which involved Eircom automatically appending telephone numbers in bulk onto other databases of names and addresses – such as direct marketing databases derived from the electoral register. This process was referred to as 'teleappending'. My Office suggested to Eircom that the disclosure of telephone directory data in this context was not a disclosure which was compatible with the purpose for which subscriber data was held by Eircom, in the absence of the clear consent of subscribers, and that the disclosure was therefore contrary to *section 2(1)(c)(ii)* of the *Data Protection Act, 1998*. In essence, I took the view that the purpose for which Eircom held the data – and which would be ordinarily understood by telephone subscribers – was the provision of a traditional 'look-up' directory service. This service was quite distinct from the population of third-party databases, which would effectively allow direct marketers to generate 'reverse-searchable' directories. In my view, such a potentially far-reaching application of personal data would need to be subject to additional clear consent from subscribers.

Following discussions, Eircom indicated its acceptance of my position on this matter, and that the practice of teleappending would be discontinued until the consent issues could be resolved. I did, however, accept that that limited forms of teleappending – for example, to update databases automatically, where an extra digit had been added to existing telephone numbers – were not incompatible with data protection law.

This case illustrates the sensitivities attaching to telephone directory information, and confirms my view that the data protection and privacy rights of telephone subscribers cannot be taken for granted. I am satisfied that Eircom appreciates this point of principle, and this is borne out by its positive response to my concerns in this case.

This case...confirms my view that the data protection and privacy rights of telephone subscribers cannot be taken for granted.

Case Study 6

Legal firm – identification of source of personal data – lack of cooperation – issue of enforcement notice

This case study provides a useful example of a matter which could have been disposed of easily at the outset, but which was protracted due to lack of cooperation from a data controller – in this case a solicitor. The case also demonstrates that, where I consider that an important issue is at stake, I am prepared to have full recourse to my legal powers until I reach a satisfactory conclusion.

The complainant had been involved in a car collision. The complainant and the other party involved had exchanged phone numbers but not addresses. The complainant subsequently received a phone call from a solicitor, acting for the other party involved, seeking her car registration number and address. The complainant declined to provide these details, since she had understood the matter to have been informally resolved, and that no recourse to legal action had been contemplated. In any event, some weeks later the complainant received a letter at her home address from the solicitor. The complainant asked how the solicitor had obtained these details, but this information was not forthcoming. The complainant raised the matter with me, as she suspected that her personal details had not been 'fairly obtained' by the solicitor, as required under the Data Protection Act.

Part Two - Case Studies

On raising the matter with the solicitor, she explained that her client had noted the registration number of the complainant's car, and that the Motor Registration Bureau had used this information to supply the solicitor with the complainant's address, in accordance with the provisions of the Road Traffic Acts. However, the complainant contested this assertion. , since the solicitor and the complainant had declined to supply this information. Why would the solicitor have requested the car registration number during their initial phone call, the complainant asked, if the solicitor's client already had this information? The complainant argued forcefully that the solicitor must in fact have obtained the data from another source.

My Office put these points in writing to the solicitor, who declined to provide any further explanation, maintaining simply that the details had been obtained from the Motor Registration Bureau. I was not satisfied with the completeness or frankness of the solicitor's response and so, after repeated refusals from the solicitor to furnish additional information, I decided to issue a formal Information Notice under section 12 of the Data Protection Act. An Information Notice obliges the recipient to *"furnish such information in relation to matters specified in the notice as is necessary or expedient for the performance by the Commissioner of his functions"*. It is an offence not to comply fully with the information sought; and in general, I only resort to issuing such a Notice if I consider that necessary information will not be provided voluntarily.

In response to the Information Notice, the solicitor stated that the details were obtained from its client and the Motor Registration Bureau. My Office then wrote once more to the solicitor expressing dissatisfaction with her reply. My Office had established that the Motor Registration Bureau had not been contacted by the solicitor until five months after the incident, while the complainant's home address was known to the solicitor within weeks of the incident. The solicitor was advised that, unless full particulars were forthcoming immediately, I would commence proceedings in accordance with section 30 of the Data Protection Act, 1988 for failure to comply with the Information Notice.

The solicitor responded with an explanation that the complainant's address details had, in fact, been obtained from her client, and only subsequently confirmed by the Motor Registration Bureau. This belated explanation, had it been provided at the outset, would have obviated the need for the protracted and time-consuming investigation of this matter.

It concerns me that, in this case, a member of the legal profession was reluctant to provide the straightforward information which I considered necessary to bring the complaint to a conclusion. It took seventeen months and the full use of my statutory powers to get the information in question. **I can ill afford the time my staff had to devote to 'delaying tactics' – but where I feel an important issue is at stake I am prepared to pursue matters fully to reach a satisfactory conclusion.** From my general experiences with legal practitioners to date, I consider this to have been an isolated case and not representative of the legal profession in general. However, should a similar type case arise in future from any source, I will have no hesitation in publicly naming the party involved, and in vigorously pursuing proceedings for any offences under the Act.

...It concerns me that, in this case, a member of the legal profession was reluctant to provide the straightforward information which I considered necessary to bring the complaint to a conclusion...

Case Study 7

Ryanair – on-line booking – delayed credit card charge – whether charge activated upon a subsequent transaction – question of disclosure of passenger data

The complainant booked an airline ticket from Ryanair, a major 'low-cost' carrier, on the internet using her credit card. However, the charge did not appear on her subsequent credit cards bills. Over ten months later, however, she booked another flight with the same airline. Her next credit card bill included two charges – one for the recent booking, and one for the booking from ten months earlier. The complainant suspected that Ryanair had associated her details with her previous booking, and had taken the opportunity to charge her credit card account for the first flight, to compensate for its own oversight. The complainant accepted that she owed the money for the first flight; but she maintained that she had given her credit card details in good faith on the first occasion, and it was hardly her fault that the airline had neglected to charge her at the time. It was not acceptable, in her view, that her credit card details – made available specifically for the second flight – should be appropriated to pay for the first flight.

The data protection issue which arose was whether the credit card data, obtained for the second booking, had been 'obtained and processed fairly' by Ryanair, as required under section 2(1)(a) of the Act. On the face of it, there was a clear suggestion that the information obtained on the second occasion was used for the purpose of a completely separate transaction.

On investigating the matter, the airline company stated that the delay in processing the payment for the first flight was due to a computer error. A batch file containing data relating to the date of the first flight, including the complainant's data, had not been sent to the bank for processing. This error was discovered some time after the event, whereupon the

...any organisation holding personal data about its customers must treat these data as being confidential - and certainly must not allow private details to be broadcast over the national airwaves...

processing of the original batch file was reactivated. This processing happened to take place around the same time as the complainant made her second flight booking. Accordingly, the fact that both payments appeared together on the complainant's credit card bill was simply a coincidence. The airline specifically denied that the data obtained on the second occasion had been used to secure payment for the first flight booking. In order to confirm this version of events, my Office contacted the bank in question. The bank provided detailed confirmation of the airline's sequence of events and established that problems had arisen with the processing of the transactions on the date of the complainant's first booking. Accordingly, I was satisfied that the complainant's concerns about possible misuse were not well-founded, and that there was no evidence of a contravention of the Data Protection Act by Ryanair in this instance.

Disclosure of Passenger Data

On a separate matter, it was brought to my notice during 2001 that a senior Ryanair representative had made comments on national radio, involving reference to named Ryanair passengers. There was a suggestion that the details might relate to a senior trade union official who bore a similar name to the passengers in question. Although I did not receive any formal complaints from individuals, I was concerned that Ryanair's public reference to named passengers appeared to be incompatible with the requirements of data protection law, and accordingly I raised the matter with the airline. Ryanair responded by noting my concerns, and by assuring me that the airline would not in future refer to any named passenger without their prior consent. While I was prepared to accept these assurances in good faith, I consider it important to emphasise that any organisation holding personal data about its customers must treat these data as being confidential – and certainly must not allow private details to be broadcast over the national airwaves.

Case Study 8

Victim Support – liaison with An Garda Síochána – disclosure of victims’ details – issue of consent

Victim Support is a voluntary organisation which provides support, comfort and counselling to people who have been the victims of crime. The organisation receives funding from the Department of Justice, Equality and Law Reform to assist in its invaluable work; but, as an independent legal entity, it is not an agent of that Department or of An Garda Síochána.

Cooperation between Victim Support and An Garda Síochána has been close. In the past, An Garda Síochána, when investigating criminal offences, had adopted the practice of automatically passing victims’ details on to Victim Support, as a means of ensuring that the organisation could contact the individuals affected, and offer their support. This practice worked well for a time, and many victims of crime benefited from the organisation’s expert and much-needed assistance. **In many cases, however, the victims were not made aware that An Garda Síochána was passing on their details in this way. In some instances, indeed, the victims in question may not have wanted their details made available to any third party, including Victim Support.** While the procedure was being applied in good faith, nevertheless I indicated that some indication of informed consent from the victim was necessary, if the referral procedure was to be compliant with data protection law. Indeed, I indicated that, in the event of my receiving a complaint from an aggrieved victim, it would be likely that I would have to rule against An Garda Síochána for incompatible disclosure of personal data. I therefore asked for the position to be reviewed, so that this excellent service might continue on a more secure and legally-compliant basis.

Some time afterwards, I was contacted by Victim Support, which expressed concern that demand for its services had fallen by about 70% in the year since automatic referral ceased. It appeared that An Garda

...I gave this matter high priority, as I was most anxious to correct any impression that data protection law was responsible for depriving victims of the benefits of the organisation’s services...

Síochána would only refer personal data to the organisation on the basis of written consent of the victim, and there were concerns that this position was unduly strict. The organisation asked for further clarification of the level of consent that needed to be obtained from victims, to allow the referral service to proceed.

I gave this matter high priority, as I was most anxious to correct any impression that data protection law was responsible for depriving victims of the benefits of the organisation’s services.

At a meeting attended by representatives from Victim Support and from An Garda Síochána, this issue was discussed in some detail. I explained that consent, at the scene of a crime, need not necessarily involve the completion of a formal consent form by a victim. In the first place, there would be no difficulty with An Garda Síochána routinely informing victims about the useful support services available from Victim Support. Moreover, victims could be informed that it was Garda policy to refer them to this organisation, if the victims were happy to indicate – whether verbally or in writing – their consent to this. Reasonable steps would, of course, need to be taken to ensure that victims did not feel coerced or pressurised into availing of the service, if they did not want to. If these elements were incorporated into Garda practice, the difficulties in routinely referring people to Victim Support, on the basis of informed consent, could be overcome to a great extent. I also indicated that the relevant Garda file, or the relevant entry on

Part Two - Case Studies

Garda "Pulse" computer system, should clearly indicate the type of consent received from the victim. Finally, I explained that if I were to receive a complaint from an aggrieved victim in the future, I would naturally be obliged to investigate it, and I would look for evidence that the necessary consent had been given, and that appropriate procedures were in place.

I am glad to report that revised procedures are now in place. I am very anxious that the victim support scheme can continue to operate in an efficient and helpful manner while at the same time respecting a vulnerable person's privacy rights. I was very heartened by and wish to place on record my appreciation of the manner in which An Garda Síochána and Victim Support responded to this delicate matter, which, I am sure, will only assist victims far better in the long run. **Nevertheless, this case highlights that - even when acting in furtherance of 'good causes' - organisations must be sensitive to people's privacy rights, to ensure that inadvertently breaches of data protection law are averted.**

...In conducting the examination, it was found that, on one of the computers, a search based upon the complainant's name gave rise to a number of apparent positive matches, which were examined further...

Case Study 9

Legal firm – registration under section 16 of the Act – on-site examination of computer files

A person complained to me that a law firm, which had processed sensitive personal data relating to her mental health, was not duly registered under section 16 of the Data Protection Act, 1988. She complained that the firm was therefore committing offences against her under the Act, and she was anxious that the firm should delete from all sensitive personal data relating to her from their computer systems.

Section 16 of the Data Protection Act requires that data controllers keeping certain kinds of personal data – what might be termed 'sensitive' personal data – must be registered with my Office in a public register, showing the types of personal data kept, the purposes for keeping these types of data, and other details. 'Sensitive' personal data includes data relating to people's physical or mental health. Failure to register, if required to do so, is an offence under section 19 of the Act. Accordingly, I took the complainant's allegation seriously and caused it to be investigated fully.

In investigating this matter, I first confirmed that there was no entry in the public register in respect of the firm. My Office then engaged in detailed correspondence with the firm to establish *inter alia*

Part Two - Case Studies

whether the firm kept personal data relating to the complainant's physical or mental health. At a meeting with the firm's Managing Partner, there was a general discussion about the issue of registration under the Data Protection Act, 1988. The Managing Partner accepted that it would be appropriate for the firm to register under the Act; and indeed the law firm subsequently registered with my Office.

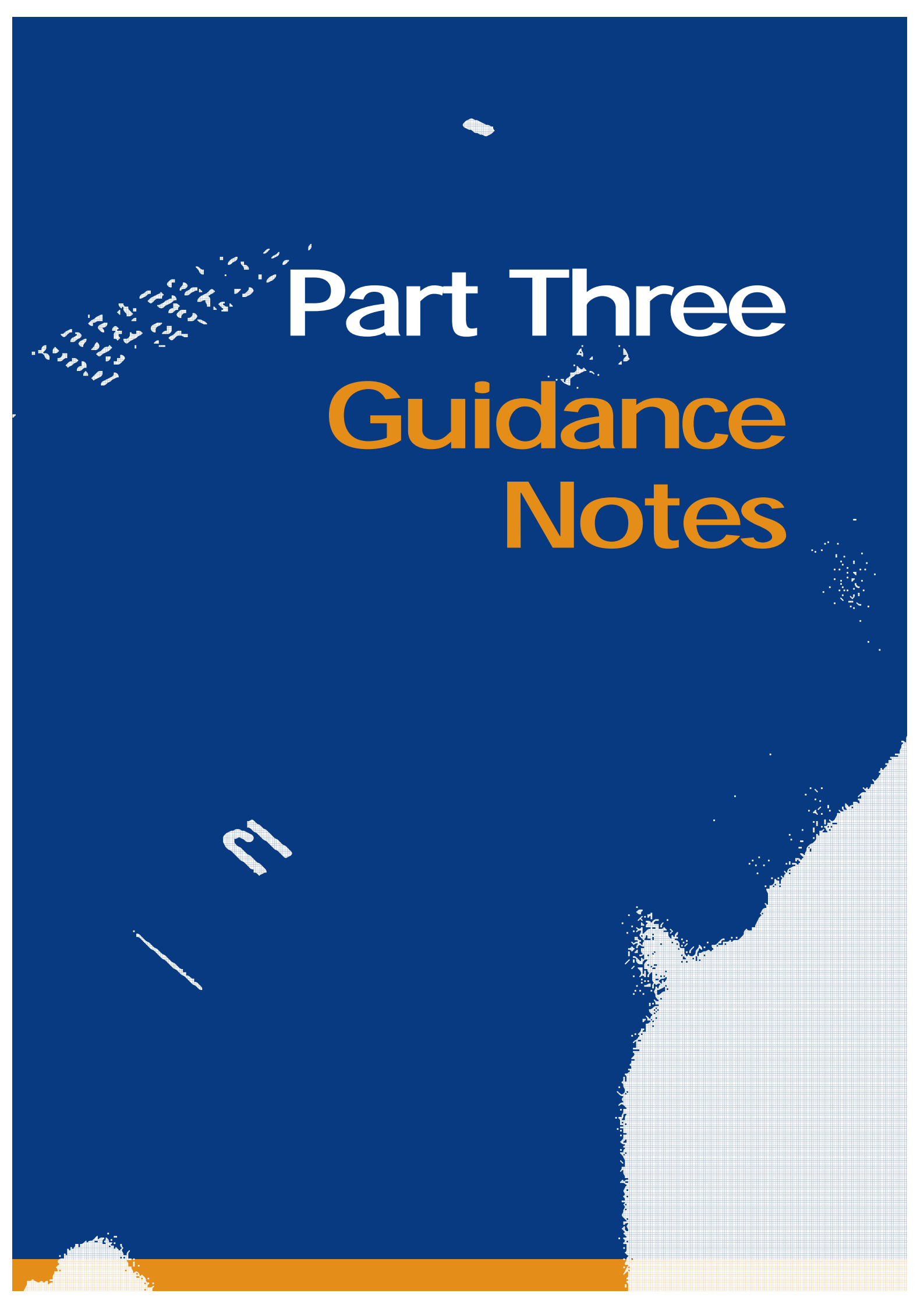
The Managing Partner also stated that his firm did not currently hold any personal data on computer relating to the complainant, and he agreed to have this statement verified by on-site inspection of the firm's computers. Authorised representatives from my Office subsequently visited the firm's offices to examine the computers for any personal data relating to the complainant. Prior to conducting the examination, the procedure which would be used for conducting a methodical search upon each computer and upon computer media was explained to the firm, and the firm co-operated fully with the examination.

In conducting the examination, it was found that, on one of the computers, a search based upon the complainant's name gave rise to a number of apparent positive matches, which were examined further. It was found that a word-processing document related to the complainant: the file related to a procedural matter about a court case involving both the complainant and a client of the firm. Further searches within the computer's e-mail application brought to light several e-mails to and from the complainant. The content of some of the e-mails was contentious or disputatious in nature, relating to a court case; but none of these e-mails appeared to contain 'sensitive' personal data. No other data relating to the complainant were found on the firm's other computers or upon its computer media.

The law firm subsequently confirmed that the personal data relating to the complainant, and found by the representatives of my Office, were held inadvertently by the firm; that there had been no intention to mislead this Office as to the existence of any such personal data; and that the personal data in question would be deleted forthwith.

I consider that the important issue raised by the complainant in this case – concerning the

registration responsibilities of a particular law firm – is of more widespread application within the legal profession as a whole. In Part 1 of this Report, I deal with this general matter in more detail.



Part Three

Guidance

Notes

Codes of Practice

While the general requirements of data protection law are quite clear, applying the rules and principles of data protection to different business activities often calls for both a knowledge of the business concerned, the data protection requirements and a degree of common sense. In addition, because the data protection rules are framed in general terms, their interpretation and application may not always be straightforward. For example, section 2 of the Data Protection Act requires that personal data must be obtained and processed *'fairly'*; that they be must not be used or disclosed in ways *'incompatible'* with the specified purpose; and that the data shall not be retained *'for longer than is necessary'*. In addition, the European Data Protection Directive, which will be implemented shortly in Irish law, makes reference to *'unambiguous consent'* as a general condition of processing personal data. It is understandable that these terms, which involve a degree of subjectivity or scope for interpretation, are liable to be interpreted differently by different people. Moreover, applying these general rules to different businesses and professions will often require a fine appreciation of the ethical norms and standards, and the traditional expectations of privacy and confidentiality, associated with that sector. The medical, telecommunications and direct marketing sectors are good examples of areas where data protection rules must be applied in a realistic and thoughtful way, drawing upon existing good practice, and sensitive to legitimate operational requirements. In short, the general nature of data protection law, to the extent that it leaves scope for doubt or ambiguity, leaves a certain deficiency in terms of legal certainty and clarity.

The *Data Protection Act, 1988* offers a solution to this difficulty through the mechanism of formal 'codes of practice'. Section 13 of the Act allows 'trade associations' or other representative bodies to prepare such codes, which would be specific to particular business sectors. Provided that such codes are approved by me as providing adequate protection for individuals – having regard to the general rules laid down in the legislation – the codes may be laid before the Oireachtas for approval. At that point, the

code will have the force of law, and will be binding upon all data controllers in that sector (whether or not they are members of the representative body). The standards laid down in the code of practice will be of crucial importance, both in the context of dealing with complaints under the Data Protection Act, and in civil actions under section 7 of the Act for a breach of the duty of care.

Advantages of a Code of Practice

To my mind, the advantages of statutory codes of practice are manifold –

- the general requirements of data protection law can be made highly specific, thus enhancing legal certainty and clarity for individual data controllers within a particular sector
- the detailed 'ground rules' will be uniformly applied to all businesses within the sector, and there will be no incentive to seek advantage by stretching or 'bending' the general rules
- moreover, the 'ground rules' can be devised and agreed by the industry itself, through its trade association or other representative bodies, on a basis that is acceptable to the Data Protection Commissioner
- finally, a more explicit set of legal rules for particular sectors will enhance people's understanding of how their personal details are handled, and of how their data protection rights can be exercised and applied.

I am disappointed that no proposal for a statutory Code of Practice has to date been brought forward by any representative association in Ireland. I anticipate, however, that the forthcoming implementation of amended data protection legislation will provide a renewed impetus in this area, by prompting data controllers to re-assess how personal data are collected and used. It is also significant that the *Data Protection (Amendment) Bill*,

Part Three - **Guidance Notes**

2002 proposes to amend section 13 of the Data Protection Act, 1988 by allowing me, as Data Protection Commissioner, to bring forward proposals of my own for sectoral codes of practice. While it is my undoubted preference for such codes to emanate from the representative associations themselves, I will certainly consider myself free to have full recourse to this new power wherever I consider that the best interests of data subjects so require. Naturally, any actions in this area would be on the basis of full dialogue and consultation with all interests affected, including both representative bodies and the public more generally.

Against this background, I consider it useful to set out now my thinking upon the elements of an effective code of practice – by which I mean a code that is likely (i) to clarify the application of data protection law, (ii) to facilitate data controllers in operating their organisations in an efficient and compliant manner, and (iii) to meet the approval of myself and of the Oireachtas in terms of underpinning people's privacy. I would also take this opportunity to encourage representative associations to consider the possibility of bringing forward new proposals for detailed codes, on the basis of the elements set out below, in order to secure for themselves and their customers the benefits of the statutory codes.

Element 1: What types of personal data are covered

The first point for decision is what types of personal data are to be covered by the code. For example, a code for GPs could usefully be confined to 'patient data', which would encompass identification details and clinical details regarding patients. Similarly, a code for the telecommunications sector should relate to 'customer data', which would include details relating to individual subscribers and 'pay-as-you-go' users. It would probably not be appropriate for either code to address 'employee data', as such a code would be more appropriate for negotiation at a more general level, i.e. by employers' representative associations, in consultation with employee interests. A telecommunications company might process a

broad range of data about its customers: from the basic (e.g. customer name and address, telephone subscriber number) to the more detailed (time, date, duration and cost of individual telephone calls made; telephone numbers called; location of subscriber). Different types of personal data will need to be subject to distinct rules in the code of practice; and indeed different categories of data subject (such as existing customer, former customer) will need different treatment. Finally, those types of personal data not listed in the code could be presumed to be 'excessive and irrelevant', in the Act's terms, in respect of the purposes governed by the code.

Element 2: For what purposes are these data processed

The Data Protection Act requires that personal data be kept for one or more 'specified and lawful purposes'. Before any assessment can be made about the latitude for processing personal data, there is a need for clarity about the full range of legitimate purposes for which the data are intended. It is useful to categorise purposes as 'primary purposes' – the purposes which are obvious to the data subject and need little explanation; and 'secondary purposes' – those of which a data subject would not necessarily be aware, unless they are brought to his or her attention. For example, a GP code of practice could confirm that patient data might be used for the primary purpose of delivering health care to the patient in question. A secondary purpose for such data might include facilitating clinical research, by making anonymised or aggregate details available to researchers or statisticians; or assisting the planning requirements of the local Health Board by providing statistical information derived from patient records. Likewise, a telecommunications code could confirm the primary purpose of providing telecommunications services to customers, and could list some legitimate secondary purposes such as: planning of network capacity; direct marketing of customers with additional services of interest; and facilitating lawful requests from An Garda Síochána in connection with the investigation of offences.

Part Three - Guidance Notes

The advantage of providing a comprehensive list of legitimate purposes is that data controllers can be assured that their existing practices are compatible with data protection law – subject to compliance with the details set out in the code – while individuals can be assured that their data will not routinely be used for other, unlisted purposes without additional steps being taken to secure clear informed consent.

Element 3: How are the personal data obtained?

Knowing what types of personal data are required, and for what purposes, it is relatively easy to ensure that the data are ‘obtained and processed fairly’, as the Act requires, and that the appropriate degree of consent has been obtained. The general, common-sense rule is that an individual’s clear consent may be taken as implicit, in the case of primary purposes – such as the provision of medical care by a GP, or the provision of telephony services (including necessary billing arrangements) in the case of a telecommunications company. Clear consent may also be inferred from a long-established course of dealings with existing customers, such as bank customers, who have not objected to certain uses of their data over that period. However, secondary uses of personal data will invariably need to be drawn clearly to people’s attention, together with an opportunity to signal consent, before clear consent for such purposes can be said to have been established. The EU Directive, with its reference to ‘unambiguous consent’ as a general rule, makes clear that positive ‘opt-in’ consent – as opposed to passive ‘opt-out’ consent – will need to be relied upon to a greater extent than heretofore.

Statutory codes can resolve ambiguities in this area by setting the parameters of when clear consent may be taken as implicit; when additional ‘opt-in’ consent is required; when ‘opt-out’ consent may still be relied upon; and when, indeed, it may be sufficient simply to inform customers that data are liable to be used for certain purposes, without a necessary requirement for consent. In determining which of these options is applicable, a data controller will need to have regard to the European Data Protection Directive’s

requirement of ‘unambiguous consent’, on the one hand; and the interplay with the alternative basis of a ‘legitimate interest’, which does not interfere unduly with the fundamental right to privacy, on the other hand. For my part, I recognise that circumstances and expectations differ widely among the different business sectors, and I am prepared to allow representative associations a certain degree of latitude in devising and setting the applicable rules – provided that the data protection and privacy rights of individuals are accorded due weight in their analysis.

Element 4: How can the personal data be processed?

To a certain extent, this issue involves a marrying of the above elements. If the personal data are of a type that is covered by the code of practice; if the purpose in question is dealt with in the code; if the use of the data for such a purpose is covered by the appropriate degree of consent – then the data may be processed in ways compatible with these elements. The advantage of a statutory code in this respect is that the subjective test of ‘compatibility’ can be codified and made concrete. For example, a telecommunications code of practice might confirm that raw telephone usage data could be processed only for the primary purpose of generating telephone bills, and for the generation of more general, aggregate data which could be applied to legitimate secondary purposes.

Element 5: To whom will the personal data be disclosed?

It is noteworthy that the Data Protection Act does not prohibit the disclosure of personal data to third parties – it simply provides that any disclosures must be ‘compatible’ with the purpose for which the data have been obtained. A code can play a useful role in making clear these ‘compatible’ disclosures. In the case of a GP, such disclosures would include locums, consultants and other persons to whom disclosure of patient data is necessary in order to advance patient

Part Three - Guidance Notes

care. Many direct marketing businesses generate income from the disclosure of databases to third parties; a code in this area could usefully elaborate upon the types of disclosure that are permissible under data protection law.

Element 6: For how long will the personal data be retained?

The rule against unnecessary retention of personal data is a key privacy protection measure, and it is essential that such a matter be dealt with adequately in a code. Again, the Act lays down the general rule – data *“shall not be kept for longer than is necessary”* for the specified purpose – and it is a natural role for representative associations, with their unique insight into operational and legal requirements within their own sector, to set more specific parameters. For example, an internet service provider might have no legitimate reason to retain records of the websites visited by individual customers, and so should delete these records as soon as practicable. A telecommunications company might need to retain detailed records of telephone usage by subscribers for a period of weeks or months, to enable routine billing queries to be addressed; while a GP might need to retain certain patient records indefinitely, to the extent that they would be relevant for future clinical use.

Summary

There are of course other important elements that should form part of useful codes of practice – factors such as security measures for personal data, updating of personal data, staff training, and organisational compliance arrangements. However, a code which is brought forward in good faith, and which attempts to address the substantive issues set out above, is one upon which I will look sympathetically. I will make every effort to facilitate representative bodies – in both public and private sectors – in devising detailed and satisfactory codes. I anticipate that the Data Protection (Amendment) Bill, 2002, with its proposal to allow me to take the first step in bringing forward

codes for consultation, will inject a new dynamic into this area of data protection law – for the benefit of data controllers, data subjects and indeed my own Office. However, I feel that the representative bodies are best placed to commence this process, and I look forward to fruitful cooperation in this area.

Considerations for the Health Sector

Introduction

Personal medical data are considered to be highly sensitive, not only for the medical information they may contain, but also because they relate especially to sensitive areas of one's private life. Increasingly, there is cross-over between GPs and other health care providers as a result of through-care and other community health initiatives aimed at continuity of care; and questions inevitably arise about patient data flows and informed consent. The doctor-patient relationship has historically been founded upon trust and professional integrity, and there is a traditional high respect in the medical profession for privacy of patients, and for the confidentiality and security of health information. Reconciling these values with the computer age, and with increasing demand from various quarters for sharing of personal health data between health care providers – in both the patients' interest and towards the wider public interest – can at times be challenging. It is for this reason that I advocate the adoption of appropriate data protection codes of practice within the distinct areas of health-care practice – ranging across the spectrum from primary care, hospitals, medical laboratories, medical research and health administration at the level of the health board.

It may, perhaps, be useful to give a general outline of the type of data protection questions that commonly arise from a health-care perspective, together with an indication the position I would adopt. These issues are ones which would lend themselves particularly well, in my opinion, to development via a formal

Part Three - Guidance Notes

code of practice. In particular, the health-care sector is one where I am very conscious that professionals themselves should take the lead in setting, and refining, the detailed standards that ought to apply, in order to balance data protection and privacy standards with the important (and sometimes, indeed, the over-riding) requirement to deliver the best clinical assistance to a patient. Accordingly, the spirit in which these 'questions and answers' are put forward is aimed at promoting reflection and informed debate within the broad health-care sector. In this regard, I recognise that – as outlined in Part 1 of this Report – the forthcoming Report of the *Health Information Working Party* may have a valuable role to play in promoting this process.

Commonly Asked Questions

Question 1: *I am a general practitioner: can my locum access my patient records?*

Yes. The Data Protection Commissioner's view is that making clinical patient records available to a locum doctor, so that the locum may provide medical care to patients, is compatible with the purpose for which the GP keeps the patient record.

Question 2: *Should my secretary or office manager be allowed access to my patient records?*

Yes, although only to the extent necessary to enable the secretary or manager to perform their functions. Non-medical professionals should have no need to access clinical material or medical notes, as distinct from administrative details (such as patients' names and addresses). The patient is entitled to an assurance that their medical information will be treated on a need-to-know basis.

Question 3: *Do I need to obtain patients' explicit permission before storing their medical details on computer?*

As a general rule, no. The patient's consent for the storage and use of their personal data is implicit in the fact that they come to you, as a medical professional, for help. However, it is good practice to inform patients that you will keep their details on computer and of what use will be made of their data. You will need to obtain clear consent for uses which might not be obvious to the patient.

Question 4: *Can I pass patient details on to another health professional for clinical purposes?*

If you are passing patient data on to a person or body acting in an agency capacity for you - such as a clinical laboratory - then this is not a 'disclosure' under the Data Protection Act, and the Data Protection Commissioner does not insist on specific patient consent in such cases. However, you should inform the patient in advance that their data will be used in this way.

If you are passing the patient data to another health professional for guidance and advice on clinical issues, the patient data should be kept anonymous unless patient identification is absolutely necessary. If you wish to pass on the full patient data, including identifying details, you will need the consent of the patient in advance, except in cases of urgent need.

Question 5: *Can I pass patient data to the Health Boards or other bodies for administrative purposes?*

You can pass on anonymised or aggregate data, from which individual patients cannot be identified. Ideally, you should inform patients in advance of such uses of their personal data.

Part Three - **Guidance Notes**

Question 6: *What if I need to disclose patient data, and I don't have the time to obtain consent?*

If patient details are urgently needed to prevent injury or other damage to the health of a person, then you may disclose the details. *Section 8(d)* of the Act makes special provision for such disclosures. However, if the reason for the disclosure is not urgent, then you will need to obtain consent in advance.

Question 7: *Can I use patient data for my own research or statistical purposes?*

Ideally you should make patients aware in advance if you intend to use their data for your own research purposes. However, the Act provides that such uses of personal data are permitted, even where the patient was not informed in advance, provided that no damage or distress is likely to be caused to the individual.

Question 8: *Can I disclose patient data to others for their research or statistical purposes?*

You may pass on anonymised or aggregate data, from which individual patients cannot be identified. Ideally, you should inform patients in advance of such uses of their personal data. If you wish to pass on personal data, including identifying details, you will need to obtain patient consent in advance. The 'research exemption', mentioned in question 7 above, only applies to your own use of personal data: it doesn't apply to disclosures to third parties.

There is an exception, however, for cancer research and screening. The *Health (Provision of Information) Act, 1997* provides that any person may provide any personal information to the National Cancer Registry Board for the purpose of any of its functions; or to the Minister for Health or any body or agency for the purpose of compiling a list of people who may be invited to participate in an approved cancer screening programme.

Question 9: *How can researchers avoid duplication of data in respect of the same individual?*

Researchers who obtain anonymised data are sometimes faced with the problem that they may be dealing with two or more data-sets from the same individual. To address this problem, it may be permissible for a data controller to make available anonymous data together with a unique coding, which falls short of actually identifying the individual to the researcher. For example, a data controller might "code" a unique data-set using a patient's initials and date of birth. The key point is that the researcher should not be in a position to associate the data-set with an identifiable individual (unless of course the individual has given clear consent for their medical data to be used for research purposes).

Question 10: *Do patients have a right to see their medical records?*

Yes they do. An individual is entitled to see a copy of any records relating to him or her kept on computer. The *Data Protection (amendment) Bill, 2002* will extend this right of access to include manual files, as required by the European Data Protection Directive.

The right of access is subject to a limited exemption in the case of health and medical records, and in the case of social worker records, where allowing access would be likely to damage the physical, mental or emotional well-being of the individual.

Question 11: *What about Medical Smart cards?*

There is no data protection objection, in principle, to smart cards which contain a person's medical history. However, it is essential in any such system that security must be robust; that data can only be read on a necessary basis; and that the data are accurate. It must also be clear who is responsible for the data – the patient himself or herself? the GP or pharmacist? the health board? the Department of Health?

Part Three - Guidance Notes

Question 12: *Have parents and guardians a right of access under data protection law to data held relating to their children?*

The right of access under section 4 of the Data Protection Act is personal to the individual in question: only that individual is legally entitled to access the data. However, under section 8 of the Act, the restrictions on disclosure of personal data do not apply in certain circumstances – including where a person is acting ‘on behalf of’ a data subject. This provision allows a data controller to provide details to a parent; but it does not require them to do so. The discretion afforded to medical professionals in this regard would need to be exercised in accordance with the requirements of medical ethics, and in accordance with any other relevant laws.

Conclusion

In addressing these and other questions, appropriate Codes of Practice for the health sector can relieve any undue concerns, and any unnecessary burden, on the part of health professionals who are anxious to comply with relevant laws. In my view, the principles of openness, transparency, fairness, confidentiality, and security are not just data protection principles – they are principles of good information management to which any organisation should adhere. When coupled with the sound principle that *“patient information should flow in parallel with patient treatment”*, suitably framed codes of practice can demonstrate how good data protection practice can facilitate, rather than hinder, effective health-care provision. I look forward to fruitful developments in this area in the future.

Appendix 1

Receipts and Payments in the year ended 31 December, 2001

2000		2001
€	Receipts	€
432,454	Moneys provided by the Oireachtas (Note 1)	524,874
311,344	Fees	341,872
1,270	Legal costs recovered	-
745,068		866,746
Payments		
307,981	Salaries & Allowances (Note 2)	362,914
19,017	Travel & Subsistence	25,214
9,696	Office & Computer Equipment	8,784
3,268	Furniture & Fittings	1,665
6,859	Equipment Maintenance & Office Supplies	12,178
9,752	Accommodation Costs ((Note 3)	26,348
18,105	Communication Costs	10,765
6,750	Incidental & Miscellaneous	22,236
35,832	Education & Awareness	54,770
6,091	Legal & Professional Fees	-
9,103	Web Site Construction	-
432,454		524,874
Payment of fees and legal refund receipts to Vote for the Office of the Minister for Justice, Equality & Law Reform		
312,614		341,872
745,068		866,746

Notes

1. Moneys provided by the Oireachtas

The Commissioner does not operate an independent accounting function. All expenses of the Office are met from subhead F of the Vote for the Office of the Minister for Justice, Equality and Law Reform. 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.

2. Salaries, allowances and superannuation

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

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

3. Premises

The Commissioner occupies premises at the Irish Life Centre, Talbot Street, Dublin 1, which are provided by the Office of Public Works, without charge. The cost to the Office of Public Works of the accommodation provided in 2001 was €63,835 ; in 2000 it was €68,497

Appendix 2

Registrations 2000 / 2001

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

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

(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
Non-associated banks	60	60
Building societies	7	6
Insurance & related services	168	164
Credit Union & Friendly Societies	448	442
Credit Reference/Debt Collection	22	22
Direct Marketing	56	57
Sub-total	799	786

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

Primary & secondary schools	26	26
Miscellaneous commercial	65	53
Private hospitals/health	99	99
Doctors, dentists, health professionals	386	425
Pharmacists	491	643
Political parties & public representatives	96	90
Religious, voluntary & cultural organisations	51	57
Legal profession	3	4
Sub-total	1,217	1,397

(d) data processors

356 390

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

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

TOTAL

2,880 3,099

Appendix 3

What's New? in the Data Protection (Amendment) Bill

The Data Protection (Amendment) Bill, 2002, contains proposals for updating data protection law, to give effect to EU standards. The main changes proposed are outlined below.

New Definitions

'Data' will include manual files as well as both computer data. This means that the scope of data protection law will extend to manual records – although the full effects of this change will not take effect until October 2007.

'Processing' is re-defined in a much broader way. 'Processing' means performing just about any operation on information or data – whether automatically or manually – such as: obtaining or keeping data; organising, retrieving, or consulting data; altering or adapting data; using, disclosing or combining the data; and erasing or destroying the data.

'Sensitive personal data', which is subject to special safeguards, is now extended to include trade-union membership data.

New Rights for Individuals

Right to Be Informed

An organisation, when obtaining personal data, must inform the individual of (i) its identity, (ii) its purpose for keeping the data, and (iii) any other information required in the interests of fairness – for example, the identity of anyone to whom personal data will be disclosed, and whether or not there is a legal obligation upon individuals to provide the data.

Organisations who have obtained personal data from a third party – not from the individuals themselves – must, in addition, contact the individuals to inform them of the types of data held, and its source.

Improved Right of Access

The right of access will now extend to both manual and computer data. In addition, a data controller must now also describe the source of the data, and the persons to whom the data will be disclosed.

Employment Rights

No-one can be forced to make an access request, or to reveal the results of an access request, as a condition of recruitment, employment or provision of a service.

Right to Object

As an individual, you may request a data controller to stop using your personal data, or not to start using the data, if you feel that the use of your data involves substantial and unwarranted damage or distress to you. This 'right to object' applies where data are being processed in the exercise of official authority, in the public interest, or for the 'legitimate interests' of an organisation.

Freedom from Automated Decision-making

Important decisions about you – such as rating your work performance, your creditworthiness, or your reliability – may not be made solely by automatic means (e.g. by computer), unless you consent to this. Generally speaking, there has to be a human input into such decisions.

New Responsibilities

Publicly Available Information

When an organisation is required by law to make a database – such as the electoral register – available to the public, such a database has, up to now, been exempt from data protection rules. The Bill restricts the exemption, so that if such a database is used for a purpose other than the purpose for which it was intended, the data protection rules apply as normal.

Legitimate Processing

In addition to the traditional rules about ‘fair obtaining’, data controllers will need to comply with additional conditions before data can be processed. In broad terms, such processing will need to be either (i) based upon unambiguous consent of the individuals; (ii) legally necessary; (iii) necessary to perform a contract to which the data subject is a party; (iv) necessary to protect vital interests of the individual, such as preventing injury, saving life, and preventing serious damage to property; (v) necessary for a public purpose, such as performance of a statutory function or a public-interest function; or (vi) necessary for a private purpose – i.e. for the legitimate interests of a data controller, provided that the fundamental right to privacy is not infringed.

Sensitive Data

In the case of sensitive personal data (such as health details, details about ethnic origin), extra safeguards must also be in place. As a general rule, explicit consent from the individual is necessary. Health professionals, who naturally need to process such sensitive details, are not subject to these extra rules.

Journalistic, Artistic and Literary Privilege

The Bill includes special exemptions for processing of personal data for journalistic, artistic or literary purposes, in order to balance the public interest in freedom of expression with data protection rights.

New Registration Rules

The existing selective system of registration will be changed: under the Bill, every data controller will be required to register, unless exempted from this requirement under Regulations made by the Data Protection Commissioner. In practice, the Commissioner will attempt to exclude as many ‘low risk’ data controllers as possible, to minimise the compliance burden on small businesses, while ensuring that the privacy interests of the public remain protected.

New Powers and Functions

Privacy Audits

The Data Protection Commissioner will have the power to carry out investigations as he sees fit, to ensure compliance with the Act and to identify possible breaches. The Commissioner intends to conduct ‘privacy audits’ upon data controllers at random, and on a targeted, sectoral basis.

Prior Checking

The Data Protection Commissioner must consider each application for registration to see whether especially risky or dangerous types of processing (as prescribed in Regulations) are involved. If so, the Commissioner must establish in advance whether the processing is likely to comply with the Act.

Codes of Good Practice

The Data Protection Commissioner will have a new power to prepare and publish ‘codes of practice’ for guidance in applying data protection law to particular areas. These codes, if approved by the Oireachtas, will have binding legal effect.