



**Data Protection
Commissioner**

An Coimisinéir Cosanta Sonraí

Annual Report

2000





**Data Protection
Commissioner**

An Coimisinéir Cosanta Sonraí

Twelfth Annual Report
of the Data Protection Commissioner

2000

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

PN. 10430

Data Protection at a Glance

Our Mission

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

What is Data Protection?

Data Protection ensures that your human rights to privacy and dignity are respected, particularly regarding the use and sharing of computer information about you. The key principle of data protection is that people should be able to control how such information about them is used - or at the very least, to know how this information is used by others.

What obligations do organisations have?

Organisations which hold computer information about individuals must ensure that the information is:

- fairly obtained and fairly used
- kept accurate and up-to-date
- secure from unauthorised access or disclosure
- kept for a clear purpose, and not used or disclosed to others except in line with that purpose
- not excessive or irrelevant for that purpose
- not kept longer than necessary for the purpose.

What legal rights do individuals have?

Individuals have a number of legal rights under data protection law. You can:

- expect fair treatment from organisations in the way they obtain, keep, use and share your information
- demand to see a copy of all computer information about you kept by any organisation
- stop an organisation from using your details for direct marketing
- demand that inaccurate computer information about you be corrected
- demand that any computer information about you be deleted, if the organisation has no valid reason to hold it
- complain to the Data Protection Commissioner if you feel your data protection rights are being infringed
- sue an organisation through the courts if you have suffered damage through the mishandling of computer information about you.

Contents

Foreword	4
Part 1 - Activities in 2000	
Introduction	8
Promoting Public Awareness	8
Enquiries	10
Complaints	11
The Public Register	13
International Activities	14
Administration	18
Part 2 - Case Studies	
An Garda Síochána	22
Department of Education and Science	24
Mobile Telephone Company	26
Irish Credit Bureau	28
Eircom	30
Financial Institution	32
Part 3 - Guidance Notes	
Introduction	36
Guidelines for the Credit Referencing Sector	36
E-Government and the REACH Project	39
Appendices	
Appendix One - Receipts and Payments in 2000	44
Appendix Two - Registrations by Sector, 1997-2000	46

Foreword

I am pleased to present this twelfth Annual Report in relation to the work of the Office of the Data Protection Commissioner since it was established in 1989. I was appointed Data Protection Commissioner in September 2000 and accordingly this annual report for 2000 also refers to matters considered by my predecessor, Mr Fergus Glavey, whose seven year term as Commissioner then concluded. I am happy to record that the work undertaken both by Mr Glavey and the first Commissioner, Mr Donal Lenihan, has enabled this office to work in a co-operative and effective manner and I intend to carry on that tradition.



The Data Protection Act, 1988 was enacted to deal with privacy issues arising from the increasing and complex amounts of information kept on computer systems regarding individuals. In giving rights to individuals, the Act also places responsibilities on those who keep personal information on computer. Soon every individual will have data protection rights extended to cover all records, including manual records, in line with EU data protection directives.

While the Act has stood the test of time to a large degree, its framers could hardly have foreseen the scale of changes that have arisen in this field in the last decade. The privacy environment for individuals is now undergoing a sea change with the increased popularity of web browsing and the era of e-commerce. Also, people are more conscious of their own privacy and are worried about the amount of data which may be held on them by state and other institutions. There is a growing demand world wide for more surveillance of people in both their private or working lives, the transfer of data by global corporations is increasing and various anti-fraud or anti-corruption initiatives undertaken can have implications for people's privacy. In addition, people are concerned about increased and unnecessary junk mail and "spam" e-mails, and about possible profiling of their behaviour and lifestyles through monitoring of their activity when they use the internet. Even though Irish organisations have on the whole exercised responsibility and care with regard to their data protection responsibilities, the global outreach of the internet means that individuals may become exposed to a wider range of data protection practices. The amount and use of data relating to

peoples' health and lifestyle are of growing concern to many individuals. Organisations dealing with sensitive health and medical issues have to be ever-vigilant in ensuring that the health data collected flows in parallel with patient treatment. Credit referencing checks and telemarketing are also on the increase while the delivery of state and private services by increased and efficient use of information technology is each day becoming more of a reality.

Many of these developments can pose particular challenges for individuals and privacy authorities world wide if they do not strike the correct balance between peoples' human right to privacy and organisations' operational requirements. In responding to these challenges I am conscious of the many fine efforts being made in general by organisations to respect data protection principles. In this regard I am strongly of the view that, far from inhibiting or curtailing e-commerce and e-Government, data protection law is in fact a key enabler because the delivery of 'e-services' depends on public credibility, first and foremost, and this Office provides a significant safeguard to people's justifiable concerns in this developing and complex environment.

At the end of the day, the common-sense principles of data protection remain the same whether services are provided online or by traditional methods. Specific "codes of practice" can assist in the task of self-regulation across the various business sectors. Such codes should be fully developed by the various service delivery organisations to take account of people's privacy rights, and I am encouraged by the responses I have received to date to my suggestions for the development of codes in particular areas. I expect to have significant progress to report on this front in the coming years.

I am also conscious of the varying requirements regarding opt-out and opt-in registers that may arise for data controllers, particularly in the area of direct marketing, with the implementation of a number of diverse national and European data protection initiatives, including:

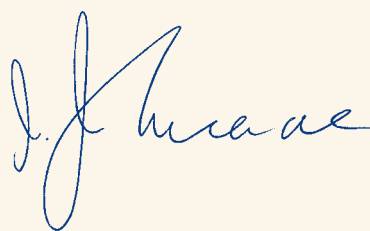
- the general requirements in the main Data Protection Directive, currently being considered by the Department of Justice, Equality and Law Reform, including the new emphasis on obtaining individuals' "unambiguous consent", and more stringent rules governing direct marketing
- the proposed provisions limiting the use of the electoral register for direct marketing, contained in the Electoral (Amendment) Bill, 2000 which was brought forward by the Department for the Environment and Local Government
- the provisions of the 1997 Telecommunications Directive, which allow for either an "opt-out" or "opt-in" system for indicating consent to unsolicited telemarketing calls, and which is now being considered by the Department of Public Enterprise
- the provisions of the 2000 E-Commerce Directive, currently being considered by the Department of Enterprise, Trade and Employment, allowing for a possible "opt-out" register for unsolicited commercial e-mail.

In my view, it would help matters for everybody if a common, coherent approach was taken by the various Government agencies as to the type of registers to be maintained, and as to the principles which should underpin them.

The year ahead year will require this Office to implement the provisions of the 1995 EU Directive on Data Protection - I understand that it will be transposed into Irish law in the near future - as well as many other duties which flow from our EU membership and other national and international obligations. These new assignments will only be feasible with increased resources as the current resources are quite inadequate to enable the Office to deliver even on its existing commitments. It is imperative that this Office responds in a timely manner to the various concerns that are brought to its attention while at the same time taking initiatives, such as privacy audits, to proactively carry out its duties. In this regard I would like to thank especially the current staff for the many efforts they have made over the past year in difficult circumstances in ensuring that the Office has worked, as far as is humanly possible, in a professional, efficient and pragmatic manner. I would also like to express my thanks to the Minister for Justice, Equality and Law Reform and his officials for the assistance given to us.

I am also pleased to record that data controllers in Ireland are, in general, quite conscious of their obligations under data protection law, although complaints and breaches can happen on occasion. It is my aim to assist controllers in their work and to try, as far as is feasible, to resolve the various disputes that can arise between data subjects and data controllers in a spirit of co-operation and mediation. However, to the extent that this approach does not prove successful, the full powers available to me under the legislation will be acted on so as to ensure that the privacy rights of individuals are fully respected.

Finally this Annual Report is the first publication from my Office to reflect the new official corporate identity and logo. The launching of this new identity is in my view timely and appropriate, reflecting the fresh impetus for data protection at this crucial stage in its development.



Joe Meade
Data Protection Commissioner

30 August 2001

Part One

Activities in 2000

The Office of the Data Protection Commissioner exercises a wide range of functions, from promoting public awareness of data protection, to investigating complaints, and liaising with international authorities. This section gives a full account of the activities of the Office during the year 2000, and gives an indication of my priorities for developing the Office into the future.

Promoting Public Awareness

The Office seeks to promote a wider public awareness and understanding of data protection matters in four ways.

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

Information booklets

My Office issues information booklets and leaflets to members of the public, free of charge and upon request. In 2000, we issued approximately 29,000 such publications. In the future, my Office will be making greater use of information technology, including the internet, to make our information more widely and conveniently available to the public. However, I anticipate that traditional printed matter - giving explanatory material simply and conveniently - will play an important role in information provision for many years into the future. Indeed, with the changes to data protection law proposed in the Data Protection (Amendment) Bill, 2001, my staff are currently redrafting and designing a new range of information booklets, and I anticipate that there will be a strong demand for these free publications.

Website information

Upon taking office as Commissioner in September 2000, I gave top priority to the development and implementation of an office website. I am delighted that my team succeeded in launching our website, www.dataprivacy.ie, by mid-December 2000.



Our Website Privacy Statement

Our website's homepage features a prominent link to our Privacy Statement, in which we assure visitors that no personal data or other technical data are recorded relating to their visit. The Privacy Statement is also linked from every page on our website. It is advisable for all organisations to have clear and straightforward privacy statements on their websites, so that people can see whether data relating to them are recorded, and how any such data are used. Privacy statements have a useful role to play in ensuring that personal data are "obtained and processed fairly", as required by the Data Protection Act.



The website provides all the essential information about data protection law and practice - from the perspective of both the individual citizen, and the organisation keeping personal data. The Office's main official publications and application forms are available to download, in addition to a range of reference material - including all of the primary and secondary legislation on data protection. My staff have already reported to me that, instead of asking for information leaflets to be posted, a growing proportion of public callers to my Office now simply ask for our website address.

In line with the Government's emphasis upon wider access to public services by electronic means, I will maintain the impetus to develop our online presence in new, more customer-friendly ways. In tandem with the roll-out of e-Government generally, my Office will seek to develop services such as online access to the public register of data controllers and data processors, and online applications for registration - including online processing of registration fees.

Media advertising

Last year my Office spent almost £28,000 on media advertising. This expenditure was targeted at a broad range of publications, ranging from standard public reference books (such as the phone book) to newspapers, magazines and specialist publications.

In the year ahead, I envisage that a significant increase in media advertising will be necessary, to publicise the new legislative provisions, and inform the public about its provisions. I will also be considering extending our advertising strategy to a wider range of media, such as the broadcast media and indeed the internet.

Direct contacts

Talks and presentations

My staff and I devote a significant proportion of our resources to giving presentations to particular groups on the application of data protection law to their area. For example, my staff gave presentations to students of direct marketing at Dublin Institute of Technology, and to medical and health sector professionals at the Royal College of Physicians in Ireland. My Office also made a presentation to the Community Relations division of An Garda Síochána, at their request, on passing crime victims' details on to the Victim Support organisation in a way that complies with data protection law. I also gave TV and other media interviews, when launching our Office website.

Working Groups and Other Fora

My Office is represented on the Internet Advisory Board, which is established to advise the Government on policy matters concerning the internet, including the prevention of illegal and

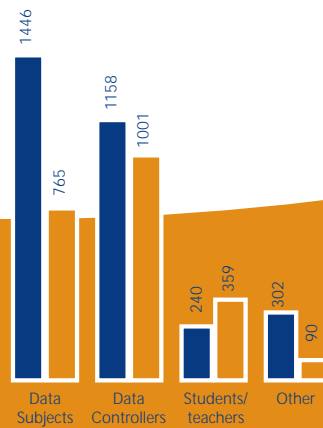


Figure 1
Contacts, sorted by category

● 2000 ● 1999

harmful use of the internet, and the promotion of responsible internet practices. The Board has liaised with the internet service industry to promote a code of practice in this regard, and has had discussions concerning the need to combat "cybercrime", and the policy and legal issues arising in this regard.

My Office was also represented in 2000 on the Health Information Working Party, an ad hoc group convened by the Department of Health and Children to discuss standards for handling medical data in the health sector. I believe there is a pressing need to rationalise and harmonise, on a sector-wide basis, the practices for handling sensitive data concerning people's health. All participants in the sector - from GPs and hospitals, who deal directly with patients, to medical laboratories, health board and Departmental administrators - need to have a clear and common understanding about how data protection rules are to be applied in this context. I am encouraged that this need now seems to be recognised, and that there are initiatives under way - from the health boards in particular - towards the development of a health sector code of practice.

Enquiries

The greater part of the day-to-day work of my Office involves responding to requests from the public for information and guidance on data protection matters. I think it is fair to say that, under my predecessors as Data Protection Commissioner, the Office has gained a high reputation among the public, and in particular among those who contact us regularly on data protection matters, for the standard of public service provided. My team endeavour at all times to be clear, straightforward and helpful, and this public service ethos is one that I intend to continue and build upon in the future.

The statistics given for 2000 as outlined in **figure 1** (above) show a significant increase in the level of queries raised with my Office from the general public. Over 1,400 contacts were received from data subjects in 2000, very nearly a doubling over the previous year.

The majority of these contacts concerned requests for general information about data protection (**figure 2**). Where more specific issues were raised, the questions of making an access request, checking a credit record, and direct marketing featured prominently.

The number of data controllers seeking information about data protection increased by about 15% over 1999, to reach 1,158 in the year 2000. This figure includes many queries from solicitors or other professional advisers on behalf of data controllers. In addition to requests for general information on meeting data protection responsibilities, specific

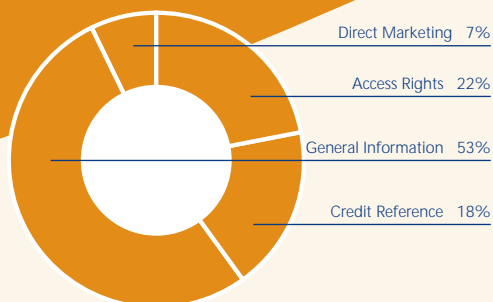


Figure 2
Data subject queries, sorted by topic

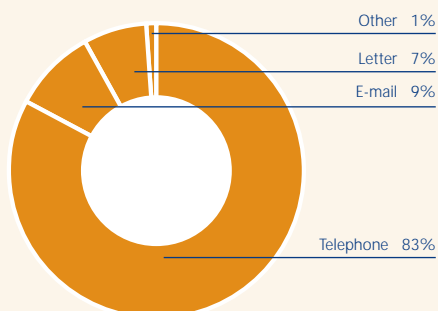


Figure 3
Contacts, sorted by contact method

topics most commonly raised included: registration with the Data Protection Commissioner; the implementation of the EU Data Protection Directive; international transfers of personal data; and responding to access requests from individuals.

Of those who contact my Office, the vast majority do so by telephone, with smaller but increasing numbers using e-mail, letters, and other methods (**figure 3**). In future years, I will also include statistics for website "hits", to give a fuller reflection of the various ways in which my Office disseminates information.

Complaints

Section 10 of the Data Protection Act, 1988 requires me to investigate complaints from individuals who feel that their data protection rights have been infringed, and to issue a decision on such complaints. My decision is subject to a right of appeal by either party to the courts.

Investigation and resolution of complaints is the primary means by which people can have their data protection rights upheld. Accordingly I attach great importance to fulfilling this statutory responsibility. Dealing with complaints is by its nature a highly resource-intensive exercise, and the additional staffing resources, which are expected to be allocated to my Office in the near future, will therefore be absolutely essential if I am to be in a position to process and finalise complaints effectively and speedily. The public are entitled to nothing less.

In 2000, the number of complaints processed formally rose to 131, relative to 105 in 1999.

Figure 4 (below) gives statistics on the level of complaints received, and the rate of processing

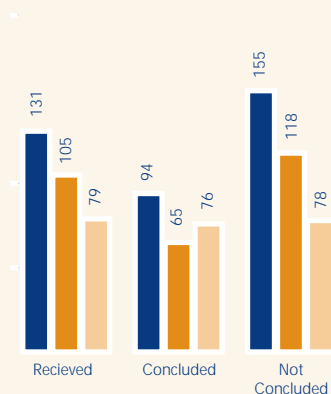


Figure 4
Complaints received, concluded and not concluded

● 2000 ● 1999 ● 1998

complaints, in the past three years. These figures clearly indicate that there is a significant increase in the volume of complaints dealt with by my Office. The figures for "complaints not concluded" have obvious implications for the level of staffing available in the Office. When a given number of staff are working to full capacity, an increasing level of complaints will naturally lead to an increasing backlog of cases. This effect is compounded by the increasing complexity and sophistication of the issues facing my Office. Indeed, matters look set to become still more complicated with the introduction of the new data protection legislation.

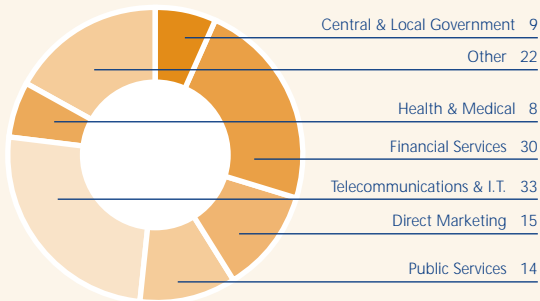


Figure 5
Breakdown of Data Controllers by business sector

Figure 5 (above) shows a breakdown of the types of organisation against which complaints were made in 2000. The telecommunications and information technology sectors account for the largest single block, with complaints typically involving concerns about the use of ex-directory information and unwanted direct marketing communications. Complaints against data controllers in the financial sector often concern the accuracy of personal data held, particularly in cases

where there is an adverse effect on a person's credit rating. As regards the other sectors, a broad range of issues have been raised, ranging from apparent failure to respond to a subject access request, to the questions of fair obtaining, use and disclosure of data. **Figure 6** (below) gives an overall breakdown of the types of data protection issues raised.

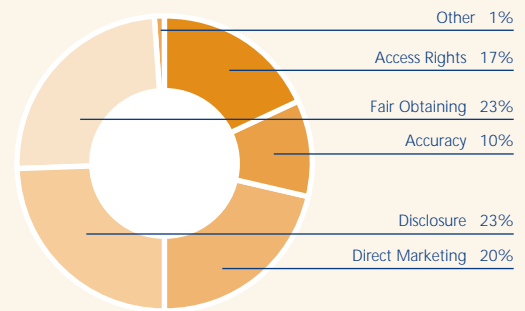


Figure 6
Breakdown of Complaints by Data Protection Issue

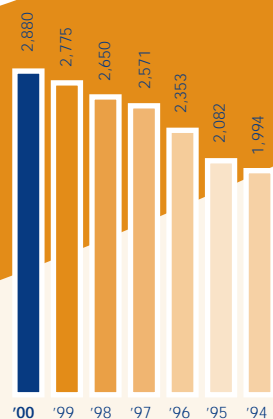


Figure 7
Number of Registrations

The Public Register

The public register of data controllers and data processors included 2,880 entries at the end of 2000, compared with 2,775 at end-1999. **Figure 7** gives an indication of the increasing numbers of registrations over recent years. Appendix Two gives a detailed breakdown of the registered data controllers by business category.

The trend in the level of registered data controllers and data processors continues upwards. With the expected transposition of the EU Data Protection Directive into Irish law, it is likely that a broader spectrum of organisations will need to register. My Office will take practical steps to give clear guidance to businesses and other organisations about how any such changes may affect them.

The Public Register

What is the Public Register?

All organisations who keep personal information on computer are bound by the data protection rules. In addition, some of these organisations are required to have an entry in a public register which is maintained by the Data Protection Commissioner.

What is the purpose of the Public Register?

The Register ensures that organisations are open and transparent about the way in which they handle personal data. In its register entry, an organisation must describe the types of personal data kept, the purposes for keeping the data, and the persons (or types of person) to whom the data can be disclosed. Once these details are set out in the register, an organisation may not use or disclose personal data in a different way. Any member of the public can inspect the register by calling into the Office of the Data Protection Commissioner.

What organisations need to register?

Broadly speaking, all public service organisations need to register, along with financial institutions, insurance companies, direct marketers, credit rating agencies, and debt collectors. Persons holding "sensitive" data, such as medical details, ethnic data, or political opinions, also need to register. As from January 2001, telephone companies and internet access companies, which keep data about individual subscribers, must register.

International Activities

Given the global reach of the internet, and the multinational dimension to business life, it is not surprising that data protection has taken on an increasingly global aspect. Data protection is not intended to restrict or hamper international affairs. On the contrary, data protection legislation was originally introduced to provide a sound basis for international transfers of personal data. This is one instance of the general principle mentioned in my Introduction to this Report, whereby data protection is to be seen as an enabler rather than an obstrucater of legitimate business activity.

With the application of the new rules on international transfers of data arising from the implementation of the EU Data Protection Directive, I appreciate that those doing business internationally will need the new rules to be applied in a clear, coherent and common-sense way, that is fully respectful of people's privacy rights. In my dealings with data controllers domestically, and in my EU and other international dealings, I will undertake to keep these standards as guiding principles at all times.

Article 29 Working Party

The Article 29 Working Party met regularly during 2000 and my Office participated in all of these meetings. Among the matters of interest discussed during the year were the following.

The Article 29 Working Party



The Article 29 Working Party is a group of all the EU Data Protection Commissioners, together with a representative of the EU Commission, which advises upon the implementation of the EU Data Protection Directive, 95/46/EC. The Working Party is established under Article 29 of the Directive. The Working Party helps to ensure that data protection issues are dealt with in a uniform way across the EU, and it advises on the data protection standards in place in countries outside the European Economic Area (EEA).

WEBLINK: A full list of the publications of the Article 29 Working Party, including the text of the various Opinions and Recommendations, can be found on the EU commission website at the address:
http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs.

Safe Harbour Agreement

The EU Data Protection Directive provides that transfers of personal data outside of the European Economic Area (EEA) to a "third country" may not, in general, take place unless the third country provides an adequate level of data protection. As the USA does not have federal data protection legislation comparable to that in the EEA, the EU Commission engaged in detailed negotiations with the US Department of Commerce towards what has become known as a "Safe Harbour" Agreement, to facilitate transfers between Member States and the USA. Under this scheme, US companies would voluntarily sign up for a code on good data protection practice, and agree to be bound by its provisions.

The Article 29 Working Party was called upon during 1999 and 2000 to provide opinions upon the various drafts of the Agreement, and this issue accounted for a significant part of the Working Party's deliberations. The comments from the Working Party were comprehensive, constructive and critical, and in my view contributed to the rigour and usefulness of the final agreement.

Eventually, in July 2000, the Safe Harbour Agreement was recognised by the EU Commission as providing "an adequate level of protection for personal data transferred from the Community to organisations established in the United States". The Agreement became operational in October 2000. More details about the Agreement, and a list of US companies who have signed up to its provisions, may be obtained at the US Department of Commerce website, www.export.gov/safeharbor. The EU Commission website also provides useful information, at the address:

http://europa.eu.int/comm/internal_market/en/dataprot/news/safeharbor.htm

Model Contracts

Where a third country does not have national data protection in place, an alternative means of ensuring that an adequate level of data protection applies, in the context of an international transfer of personal data, is to include appropriate provisions in the contract which governs the transfer operation. The EU Commission has devised draft "model contracts" which could serve such a purpose, and the Article 29 Working Party offered feedback on the adequacy of the terms of these draft contracts. Indeed, the draft contracts have since been finalised and are available for inspection at the EU Commission website, at the address quoted above.

Approval of Third Countries

Where a third country does have data protection legislation in place, the Article 29 Working Party must give an opinion regarding the adequacy of the legislation. In 2000, the EU Commission confirmed that the systems in place in Switzerland and Hungary were adequate, on foot of recommendations to this effect from the Working Party.

Reverse searching using public telephone directories

The Article 29 Working Party made clear that reverse searching using electronic versions of the public telephone directory, in ways not authorised by subscribers, was contrary to data protection norms. The opinion fully reflected Irish experience of this matter, as outlined in Case Study no. 8 in last year's Annual Report.

Data Protection and the internet

The Article 29 Working Party produced a document setting out the application of data protection to the internet environment, and drawing attention to some privacy issues and challenges unique to this environment.

The Human Genome project

The fundamental privacy issues arising in the context of the mapping of the human genome were commented upon by the Working Party.

Supervision of Europol and other "Third Pillar" bodies


The Europol Joint Supervisory Body (JSB) meets on a quarterly basis to discuss issues relating to the data protection supervision of Europol. Matters discussed in 2000 included the terms of "opening orders" which authorise Europol's opening of analysis files on particular topics, and giving views on whether the data protection standards in third countries are sufficient to enable data sharing negotiations to begin. One important discussion point in 2000 was the creation of a dedicated, independent secretariat to facilitate the work of the JSB and other third pillar bodies, such as the supervisory authorities for Schengen and the Customs Information System (see below). Discussions on this matter culminated in agreement and the new secretariat will be in place from September 2001.

My predecessor as Data Protection Commissioner, Mr Fergus Glavey, stood down as Chairman of the JSB in 2000, having served in that capacity for two years. As the first Chairman of the JSB, he contributed significantly to the work of that body, and to the standing of the Irish Data Protection Commissioner's Office. I will seek to uphold these achievements in the years ahead.

Appeals Committee

No appeals were brought before the JSB Appeals Committee in 2000.

Europol

The logo for Europol, featuring the word "EUROPOL" in a bold, sans-serif font. The letters are white and set against a dark, circular background that has a blurred, motion-like effect, suggesting a globe or a network. The logo is centered within a white rounded rectangular box.

What is Europol?

Europol, or the European Police Office, is a body to facilitate effective cooperation among EU Member States in tackling serious international crime. Europol is established under the 1995 Europol Convention. This Convention was given effect in Irish law by the Europol Act, 1997. Europol is based in The Hague, the Netherlands.

What is the Europol JSB?

Because international cooperation in combating crime involves transfer of sensitive personal data, and the maintenance of important databases, data protection safeguards have been built into the Europol Convention. An independent "Joint Supervisory Body", made up of representatives of the data protection authorities from the Member States, supervises the adherence by Europol to data protection rules.

What is the JSB Appeals Committee?

Individuals have the right to seek access to any information held about them by Europol, by applying through their national police service. Appeals against decisions of Europol in this regard are handled by a Committee of the JSB known as the Appeals Committee. Its decisions are binding upon Europol.

WEBLINK: More information about the work of Europol can be found at the website: www.europol.eu.int

Domestic supervision

One of the functions assigned to my office under the 1997 Europol Act is to act as the national supervisory body for the Europol "national unit", a unit of An Garda Síochána. Since taking office as Data Protection Commissioner, I have had detailed and most constructive discussions with An Garda Síochána in regard to this and other matters, and I envisage a continuing positive working relationship with this important "data controller" into the future.

Other Third Pillar Bodies

The "third pillar" of the EU refers to items in the area of police cooperation, home affairs and immigration. In the data protection field, the third pillar areas concern the Schengen Agreement, which allows for passport-free travel within the Schengen countries; the Customs Information System (CIS), which allows for EU-wide cooperation in dealing with customs matters; and the Eurodac system, which allows for exchange of fingerprint data relating to asylum seekers among EU immigration authorities.

With regard to the Schengen Agreement, the position is that thirteen EU Member States are party to this Agreement (the exceptions being Ireland and the United Kingdom), along with Norway and Iceland. The border-free travel arrangement is coupled with a database (known as the Schengen Information System or SIS) to counter immigration fraud. Since Ireland is not a member of the Schengen Group, my office currently has no role in the data protection supervisory body (the Schengen Joint Supervisory Authority) that supervises this database.

The CIS is established under the 1995 CIS Convention. The supervisory authority envisaged in that Convention was not active in 2000. However, with the passing of the Customs and Excise (Mutual Assistance) Act, 2001, and the designation of the Data Protection Commissioner as the "national supervisory authority" for the purposes of the Convention, I anticipate that activity in this area will get under way in 2001.

The European Regulation establishing the "Eurodac" system, enabling Member States to exchange fingerprint data about asylum applicants, was adopted in December 2000. The Eurodac system includes in-built data protection procedures and safeguards; however, since the system is not expected to become operational until 2002, there have not as yet been any practical implications for the work of my Office.

International Conferences

I attended the *International Conference of Privacy and Data Protection Commissioners*, held in Venice, Italy in September 2000. The Conference allows data protection authorities from around the world, and other interested parties, to come together to discuss developments of common interest. The 2000 Conference included important discussions on the use of genetic data, cybercrime, data matching and international data transfers.

Another long-established international forum is the *Spring Conference of European Data Protection Commissioners*, which took place in Stockholm, Sweden in May 2000. The Spring Conference is attended by Data Protection Commissioners from the whole of Europe, not just those in the EU, and is an useful forum for exchanging views and knowledge on emerging issues in the field of data protection. The 2000 Spring Conference included discussions on retention of traffic data by

telecommunications and internet bodies, video surveillance, and privacy audits.

International Complaints Handling Workshops

An example of a practical outcome from the Spring Conference is the establishment of twice-yearly workshops to discuss approaches to dealing with complaints. It had been agreed at the 1999 Spring Conference that it would be helpful to compare the different procedures in use across Europe for investigating breaches of data protection legislation - particularly in light of the greater level of harmonisation of data protection legislation on foot of the EU Data Protection Directive.

The first "complaints handling workshop" was held in Manchester, England in February 2000 and a second - attended by staff from my Office - was held in The Hague, the Netherlands in October 2000. Although still in its infancy, the structure is proving a valuable forum for exchanging information and sharing experiences on case handling. As well as compiling a list of national liaison officers, this group has also established a web-based forum for enhancing international co-operation amongst the investigation branches of the various authorities. Indeed, my Office looks forward to hosting one such workshop in March 2002.

Finally, the *British and Irish data protection authorities* (including those from the Isle of Man, Guernsey and Jersey) had two very useful meetings in 2000 to exchange information and views of matters of common concern.

Administration

Running Costs

The costs of running the Office in 2000 are as set out in Table 1. 1999 figures are given for comparison, and euro figures for 2000 are given for information.

Table 1
Costs of running the office in 2000

	1999 (IRE)	2000 (IRE)	2000 (€)	% change
Overall running costs	392,525	394,531	500,951	0.5%
Receipts	233,674	245,203	311,344	5%
Receipts as % of running costs	60%	62%		

The slight fall in overall running costs was attributable to once-off items of expenditure in the year 1999, including Year 2000 computer expenditure and certain accommodation costs, which did not recur in 2000, partially offset by increased staffing costs, travel costs, and expenditure on advertising.

Detailed figures for the year 2000 are included for information purposes in Appendix One.

Staffing

I believe it is useful to recap how the developments in the overall area of data protection, particularly over the past two years, have impacted upon the work of this Office, and to outline the direction in which the Office is headed.

There is, indeed, an entirely new working environment for the Office. In the first instance the staffing of the Office stands, at the date of this Report, at seven, compared with six when the office was established in 1989, and eight in 1995. I would re-iterate the point made by my predecessors that the staffing complement of the Office has not kept pace with the demands placed upon it. The following domestic and international developments illustrate the transformation in the data protection environment:

- the imminent transposition of the EU Data Protection Directive into Irish law
- the participation of this office in the Article 29 Working Party, established under the Directive
- the assignment of new data protection responsibilities on the Office, arising from EU initiatives in the area of telecommunications (Directive 97/66/EC), customs and excise (the CIS Convention) and, Europol, with future developments likely under the Schengen Agreement and the Eurodac regulation
- the development of complex international agreements and procedures (e.g. the EU/US Safe Harbour Agreement, the adoption of standard model contracts) to facilitate international transfers of personal data
- the increased complexity and sophistication of data protection issues, as modern

technology presents new and pressing privacy challenges - e.g. in the area of internet use, e-Commerce and e-Government, the increasingly electronic nature of large-scale and public databases, and the data matching issues that arise in this context.

As of now, the Office is quite simply not equipped to meet adequately its current responsibilities. Quite apart from the low staffing complement, the Office has experienced over recent years continual changes in personnel, whether through transfer, promotion, or resignation. While changes in personnel are a reality for most organisations, it poses significant challenges for a small Office which has to administer highly complex and nuanced legislation. Training and coaching naturally have a role to play in equipping staff with the relevant skills, but the overall staffing situation remains highly unsatisfactory.

I should add that I am encouraged by the positive response I have recently received from the Department of Justice, Equality and Law Reform to my concerns, and I expect the position to improve significantly in the coming months.

Support Services

The technological improvements introduced during 1999 as part of our Year 2000 strategy have stood the Office in good stead during the past year. I am happy to acknowledge the support provided by the IT Section of the Department of Justice, Equality and Law Reform, while its Finance Division also continued to provide my Office with an invaluable service in the area of receipts and payments.



Part Two

Case Studies

Case Study 1

An Garda Síochána - subject access request - time limit for response - accuracy of personal data - excessive and irrelevant personal data - date of birth

An individual wrote to An Garda Síochána seeking access under the Data Protection Act to all personal information held about him on computer. He gave his full name and address, and enclosed a postal order for £5.00 (the maximum fee payable for an access request). An Garda Síochána wrote back to him requesting him to specify which databases were to be checked, and requesting that he provide additional details including date of birth. In reply, the individual confirmed that all databases were to be searched, but he declined to provide further personal data, as he felt that An Garda Síochána had sufficient details to identify him. After further correspondence between both sides, the individual specified three particular databases which were to be searched, he provided his date of birth, and eventually he received a copy of the relevant records from the Criminal Records Database maintained by An Garda Síochána. The records related to a road traffic conviction in the District Court, including a record of the sentence imposed. The individual complained to me on two main grounds: (i) the delay in responding to his access request, and (ii) inaccuracy of the personal data held by An Garda Síochána.

On the latter point, the individual established that the details relating to the sentence imposed upon him by the District Court were incorrect. Moreover, his conviction at the District Court had in fact been appealed to the Circuit Court, and, while the conviction had been upheld, the sentence had been varied. These facts were not reflected in the record maintained by An Garda Síochána. When these facts were brought to the attention of An Garda Síochána, prompt action was taken to append the relevant Circuit Court details to the existing District Court data.

The complainant was not happy with this Garda response. He argued that the details relating to the District Court conviction should be deleted from his Garda record, since this conviction had been appealed and was therefore not a valid conviction. The complainant argued that the conviction in respect of which he was required to pay a fine took place at the Circuit Court, not the District Court, and accordingly the recording of information about his District Court hearing was "excessive" and "irrelevant", contrary to section 2 of the Data Protection Act, 1988.

I did not accept the complainant's reasoning on this point. In accordance with the provisions of the Courts Acts and Courts of Justice Acts, an appeal from a lower court to a higher court enables the higher court to either affirm or to reverse, in whole or in part, the conviction applied by the lower court, and to vary the penalty or sentence imposed by the lower court, as the case may be. Accordingly, I did not accept the complainant's contention that his conviction before the District Court was not valid. In fact, the conviction of the District Court had been affirmed by the Circuit

Court, although the original penalty and expenses imposed upon the complainant as a result of this conviction had been varied by the Circuit Court.

In light of this finding, I considered it appropriate for An Garda Síochána to record full and accurate particulars in relation to that conviction on its Criminal Records Database, provided that the outcome of the appeal hearing was also accurately recorded. However, I upheld the complaint that the information kept on the database had been inaccurate at the time An Garda Síochána responded to the access request. In my Decision on this matter, I noted that the details held on the Criminal Records Database are of a unique and particularly sensitive nature, and have the potential to reflect upon an individual's personal character in a profound manner; and the care taken over the accuracy of records on this database should be set at an appropriately high level.

As regards the length of time taken to respond to the access request, I noted that An Garda Síochána responded to the access request within the statutory maximum period of 40 days from the time of receiving the details they had requested from the complainant, and accordingly I did not uphold this element of the complaint. It should be noted that the 40-day period does not always start at the time the individual first writes to a data controller. If the data controller has doubts about the identity of the requester, or has insufficient details to locate the necessary records, then it is entitled to revert to the data subject seeking clarification on these points.

Some points that were made clear in the context of this complaint were the following:

- As a general rule, where a data controller has two or more databases, it must treat a subject access request as relating to all of these databases, unless the requester indicates otherwise. A data controller

cannot delay the processing of a request simply to seek specification of which database is to be searched. An exception to this general rule arises when a data controller opts to have separate register entries in respect of distinct databases (as provided under section 17(1)(b) of the Act). In such cases, requesters may be asked to specify which of the registered databases are to be searched, and may be asked to pay a separate fee for each one.

- Where an individual wishes all databases to be searched, he or she must provide all of the information necessary for the searches to proceed. While I do not accept that a requester's date of birth is routinely needed to establish his or her identity in all cases, I do accept that the date of birth may be helpful in verifying identity in cases of doubt, and that it may be necessary to enable searches to proceed upon large databases which are searchable according to name and date of birth. The date of birth may also be necessary to distinguish individuals of similar name.

Case Study 2

Department of Education & Science - use of trade union membership subscription data to withhold pay - fair obtaining and processing - specified purpose - compatible use - purpose as described in register entry

A group of teachers, all members of a particular trade union, was engaged in industrial action against the Department of Education & Science. The Department decided to withhold pay from the individuals for days on which, arising from their industrial action, the individuals were not - in the view of the Department - properly performing their work duties. In order to do this, the Department used the payroll database to identify those individuals who were members of the trade union, and pay was withheld from those individuals.

A number of the teachers affected complained to me that the use of their personal data in this way was contrary to the Data Protection Act. Many of the complainants said it was wrong that information held by the Department in order to facilitate the deduction-at-source of union subscriptions should be used for this new purpose, against their interests and without their consent or authorisation. Some individuals pointed out that,

while they were members of the trade union, they had in fact been working normally on the days in respect of which the pay deductions were made.

I raised this matter with the Department, which responded promptly and seriously, and it was agreed that no further deductions would be made pending the resolution of the data protection issues. For my part, I made it plain that my investigation had nothing whatever to do with the substantive industrial relations issue of whether the Department had the right to withhold pay, but only with the question of whether the means used to achieve this end were compatible with data protection law.

Section 2 of the Act provides that personal data "shall have been obtained, and shall be processed, fairly". That section also requires that the personal data "shall be kept only for one or more specified and lawful purposes", and "shall not be used or disclosed in any manner incompatible with that purpose or those purposes". Taken together, these provisions amount to a general requirement that individuals should be made aware, at the time of the collection of their personal data, of the purposes to which their data will be put, and that the data may not subsequently be used for different purposes, without first obtaining the authorisation of the data subjects. I share the view consistently and clearly expressed by my predecessors that this simple principle of fairness and transparency is the very bedrock of data protection law.

In the case in question, I noted that the complainants had provided their trade union membership details on a special authorisation form,

titled "Authorisation of Deduction of Subscription from Salary". The wording of the form simply mandated the Department to deduct union membership subscriptions from salary, and forward the moneys to the trade union. The form made no mention about other uses by the Department of the individual's trade union membership data. In these circumstances, I was satisfied that the purpose for which the data had been obtained by the Department, and for which the data were kept, was quite plain; and that this purpose did not encompass the use to which the Department had actually put the data.

Against this, the Department argued that the terms of its register entry were sufficient to authorise the use of the personal data in these cases. One of the Department's entries in the public register described the "purpose" of holding personal data as: "Administration of teaching staff for second level schools." The data in question were described in the register entry as including "payment matters." The Department argued that the "specified and lawful purpose" referred to in section 2 of the Act must be determined by reference to the purpose set out in the register entry. Since the withholding of the complainants' pay came within the scope of the broad purpose "administration of teaching staff", the Department argued that its use of personal data was "not incompatible" with that broad purpose, and so no contravention of the Act was involved.

This argument was not one I could accept. I explained that the "specified and lawful purpose" mentioned in section 2 of the Act is to be determined by reference to the circumstances in which data have been obtained. Since the personal data relating to trade union membership had been obtained via a deduction-at-source mandate form, and accepted on that basis, then the "specified and lawful purpose" for holding those particular data related to the deduction-at-source facility, not any

...the "specified and lawful purpose" mentioned in section 2 of the Act is to be determined by reference to the circumstances in which data have been obtained...

other purpose. This purpose should have been reflected in the Department's register entry. In fact, the Department had included a much broader description of purposes in its register entry. The Department could not legitimately rely upon this broad description to displace the actual purpose for holding the union membership data, or to infer the existence of new "specified and lawful purposes" which were unknown and unthought-of when the data had been obtained. As my predecessor commented when this argument was discussed in a previous case (case study 8 from the 1998 Annual Report):

The purpose of including details in the Register entry is to describe, in a publicly accessible form, the outer limits of what the data controller may do with personal data, not to provide a 'back door' that would allow a data controller to circumvent its basic data protection responsibilities.

I accordingly decided that the Department had breached data protection law by using the complainants' trade union membership data as it had.

Since this case was concluded, I have contacted the heads of all Government Departments, advising them to ensure that the details recorded in their public register entries are appropriately detailed, meaningful and specific. In this way, there can be clarity on all sides regarding the uses to which personal data may legitimately be put.

Case Study 3

Mobile telephone company - subject access request - commercially sensitive information

The complainant in this case had difficulty when he attempted to purchase a mobile telephone from a shop. The shop took his details on a sign-up form, and telephoned the mobile phone company to activate the service, which was to operate on a contract basis. The mobile telephone company declined to accept the complainant as a customer, and refused to give reasons. When the complainant pressed the matter, the mobile telephone company said they would only provide a service if he made a deposit of £100.

The complainant made an access request under section 4 of the Data Protection Act, asking to see a copy of everything held on computer about him by the mobile telephone company. The company responded by giving him a summary of the types of information they kept about him, and assuring him that the only details they kept were those which the individual had provided on the sign-up form. They indicated that these details had been subject to an assessment procedure known as "credit scoring", and this was the reason for the requirement that he pay a deposit. The individual was not satisfied to receive summary information, rather than a full copy of the computer data relating to him, and so he complained to my Office.

...the individual had a clear legal right to see a copy of all the information relating to him. The exceptions to the right of access, set out in section 5 of the Act, did not include any reference to "commercially sensitive information"...

It was agreed that my staff should visit the premises of the mobile telephone company to see exactly what personal data were held. The company's computer system was shown to my staff. The company explained that printing off a copy of the information which they held on computer would identify the software package in question, and this was in the company's view commercially sensitive information. In response, my Office pointed out that the company was free to take any reasonable steps to hide the identity of the software package. However, the individual had a clear legal right to see a copy of all the information relating to him. The exceptions to the right of access, set out in section 5 of the Act, did not include any reference to "commercially sensitive information". The point was also made that, just because the complainant might already have the details in question, this was no ground for refusing to comply with a valid access request. After consideration, the company agreed to forward a full copy of the personal data to the complainant.



...the general practice of providing "close matches", runs the inevitable risk of disclosing people's confidential financial details to institutions which have no business in seeing these details ...

Case Study 4

Financial institutions - Irish Credit Bureau - credit referencing - incompatible disclosure - "close matches"

An individual made an access request to the Irish Credit Bureau (ICB), the main credit referencing body in Ireland, to see his credit record. On receiving the information, he noticed that a number of financial institutions, with which he had never had any dealings, had viewed his credit record. The individual was concerned that his private financial affairs had been disclosed in contravention of the Data Protection Act.

In the course of our investigations into this matter, my Office established that the financial institutions involved had made a credit check relating to another individual who shared a similar (but not identical) name and similar (not identical) address. The ICB returned information relating to the complainant, on the basis that his details were a "close match" to those supplied by the financial institutions. The ICB defended this practice, arguing that, in the absence of a unique personal identifier or precise postal codes, and in the light of Gaelic name variations, determining identity with precision was not an exact science in the Irish context.

While noting the general point made by the ICB, I did not see that there was any justification for the supply of data relating to the complainant in this

particular case. Certainly, the financial institutions which had been given the complainant's details were able to discern that information had been "over-supplied", and could identify and dispose of the information relating to the complainant. The real issue in this case was a procedural one, as to whether sufficient effort had been made by the ICB to ensure that financial institutions were supplied with personal data relating only to those people who had applied to them for credit. The facts in this case indicated to me that there was room for, and a necessity for, improvement in this regard.

The incidents in this case occurred a number of years ago, and since then the ICB has endeavoured to upgrade its procedures. However, it is clear to me that the general practice of providing "close matches", and leaving it up to financial institutions to identify and discard excessive information, runs the inevitable risk of disclosing people's confidential financial details to institutions which have no business in seeing these details. Accordingly, any such practice will fall foul of data protection law. My views on the correct standards of data protection that should apply in the credit referencing sector are set out in some detail in Part 3 of this Report.



Case Study 5

Eircom - ex-directory telephone customers - proposed disclosure to other telecommunications companies - limited use of ex-directory customer data - compliance with decision of ODTR

Eircom, a telecommunications company, maintained a large database of its telephone subscribers, some of whom were ex-directory. In the context of providing directory enquiries services, the company included the name and address of ex-directory subscribers, although the telephone number was blocked. Other telecommunications companies were allowed access to the Eircom subscriber database for the purpose of providing competing directory services, but data about ex-directory customers was withheld. The competing companies protested to the Office of the Director of Telecommunications Regulation (ODTR) that the withholding of ex-directory data, and its limited use by Eircom for directory services, was unfair and anti-competitive. The ODTR, having considered the matter and consulted with this Office, held (in its Dispute Resolution Determination Number 03/00) that Eircom was correct to withhold ex-directory data for reasons of data protection law, but that Eircom should make no use of the ex-directory data

in its own directory service - thus maintaining a level playing-field with its competitors in this business. ODTR also observed that consumers' best interests would be served by providing them with a wider range of options regarding the uses of their personal data.

Subsequently, in October 2000, Eircom issued a mailing (by open postcard) to its ex-directory subscribers, informing them that their names and addresses, but not their telephone numbers, would be passed to other telecommunications companies for the purpose of providing directory information services. The mailing also said that subscribers had a right to have their personal details excluded from such directory information databases.

This mailing gave rise to confusion and concern among some subscribers, who complained to me that their data protection rights were being undermined. I raised the matter immediately with Eircom, which explained that it was attempting to comply with the ODTR decision, particularly with regard to widening the choices of subscribers about the uses of personal data. However, I pointed out that the mailing did not appear to meet this objective. The mailing simply informed ex-directory subscribers that their personal data would be disclosed to third parties and that subscribers could opt out of this practice by writing to Eircom. In my view, any such disclosure would be in breach of the Data Protection Act, in the absence of the positive consent of subscribers. I also expressed the view that mailings of this nature should not take place by way of open postcard.

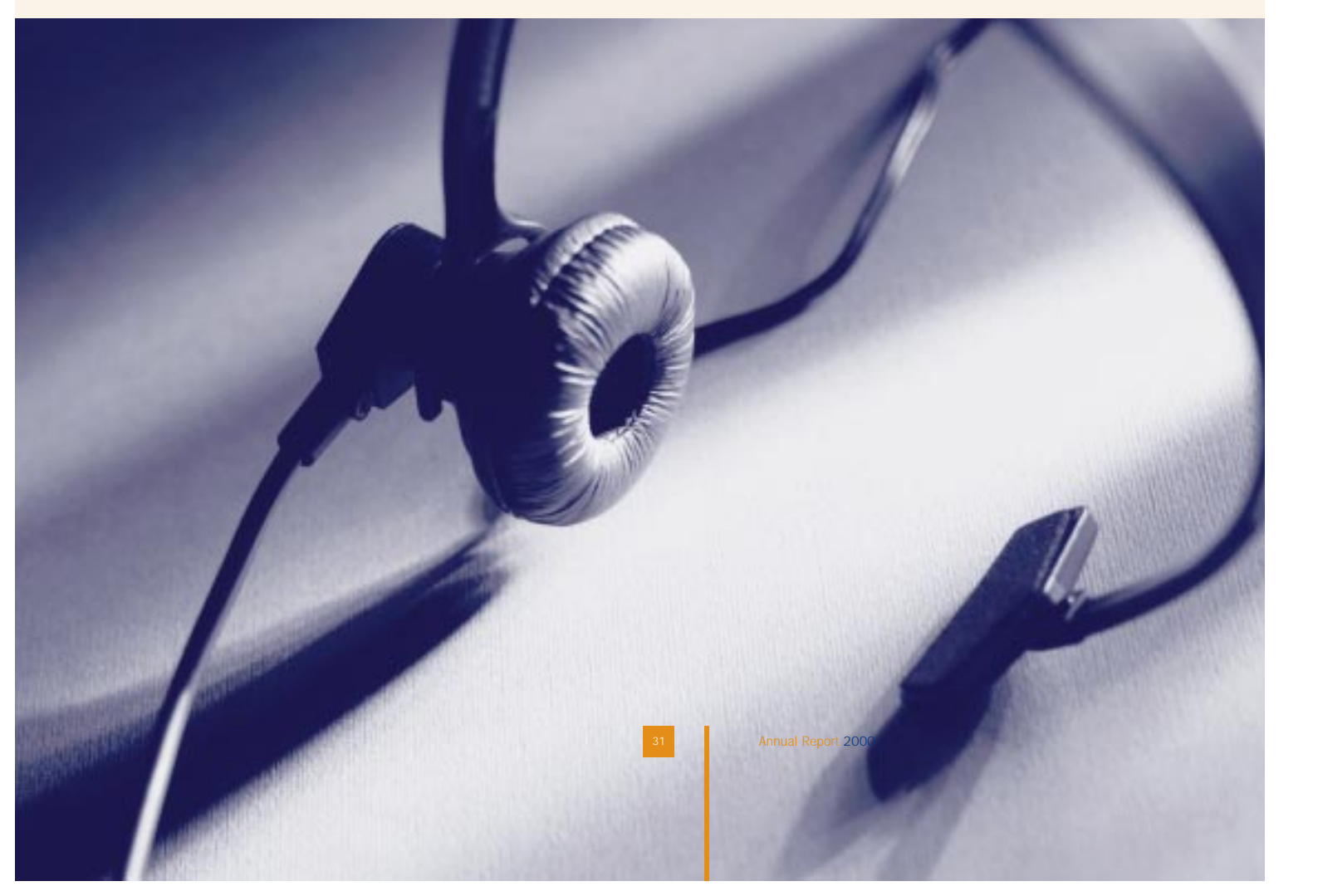
Following these discussions, Eircom undertook not to issue any further mailings about the proposed

... The mailing simply informed ex-directory subscribers that their personal data would be disclosed to third parties and that subscribers could opt out of this practice by writing to Eircom. In my view, any such disclosure would be in breach of the Data Protection Act...

disclosure; not to disclose ex-directory subscriber data to other telecommunications companies; and confirmed that such data would not be used in Eircom's own directory enquiries service.

I consider it appropriate to point out that, despite the confusion that arose in this instance, Eircom has on the whole shown itself to be a responsible and conscientious data controller, which takes its data protection obligations quite seriously as a general

rule. More generally, the Directory Information Services Forum (DISF), a discussion group convened by the ODTR, has recently made welcome progress in laying down guidelines for the responsible use of the National Directory Database, the principal telephone directory which will include the directory listings from all Irish telecommunications service companies. I am happy to record that there is an increasing acceptance among telecommunications companies that the provision of services to subscribers, and commercial services using subscriber data, needs to be based upon the fundamental principle of subscriber consent. Indeed, the solid assurances on this front arising from the DISF initiative and other initiatives may, in my view, lead to a reduction in the high proportion of subscribers in Ireland who choose to have ex-directory status.



...personal data, stored in debit cards, credit cards, and indeed in any type of card using a magnetic strip or similar storage mechanism, should be kept secure from inappropriate disclosure...

Case Study 6

Financial institution - Laser card - printing of home address on receipts - incompatible disclosure - adequate security

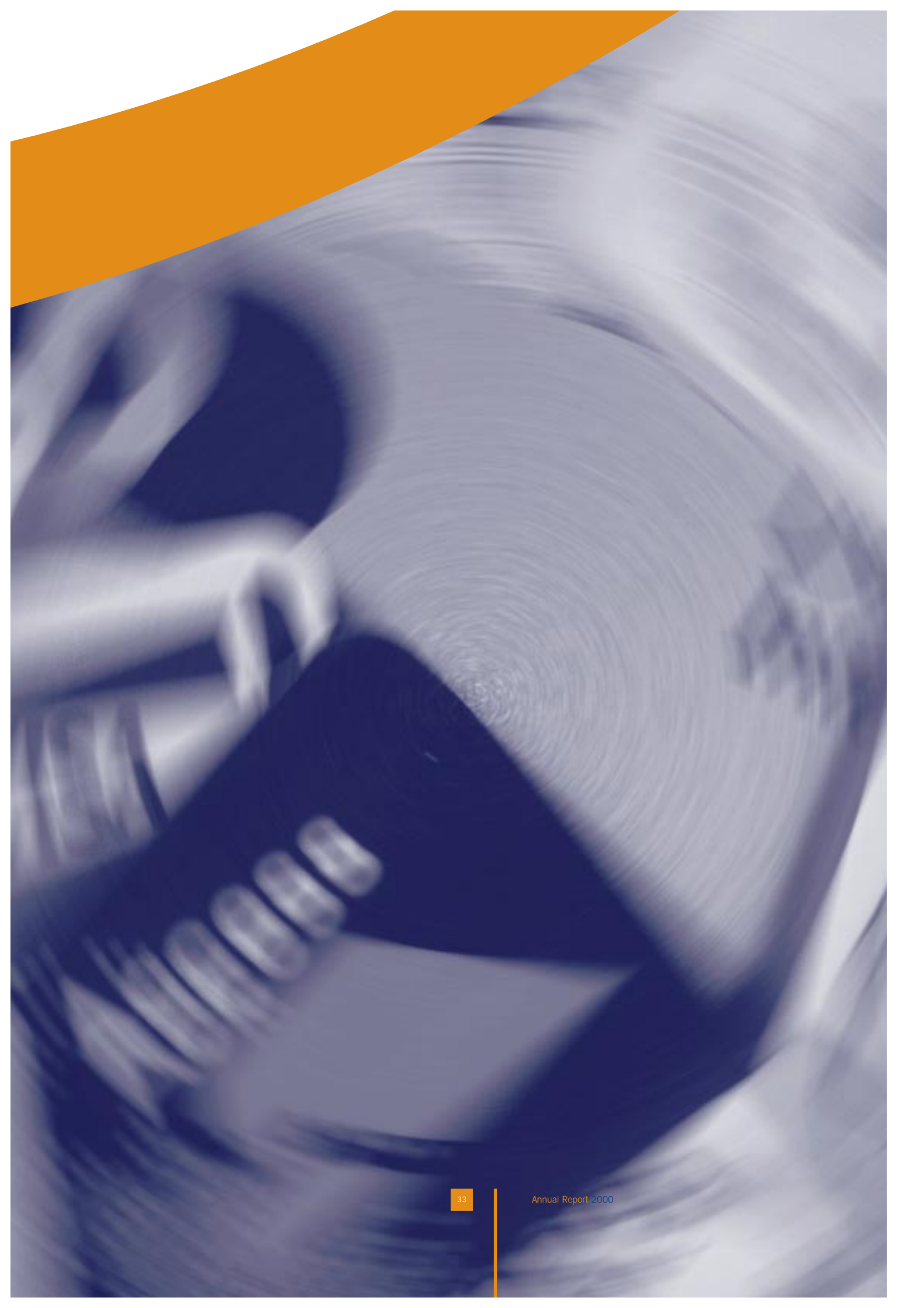
An individual wrote to me expressing his concern that when using his Laser card - a type of debit card that can be used in shops for cashless transactions - his home address was printed on the receipt slip. Since retailers keep a copy of the receipt slip, the individual felt that his private details were being disclosed unnecessarily by his financial institution, which was responsible for the Laser card.

My Office raised this matter with the financial institution, which responded promptly to the matter. The institution indicated that it had itself received a small number of complaints from customers about this matter. The institution explained that Laser cards issued after October 1999 included the customer's home address details in the magnetic stripe. However, these details were only supposed to be read by automated lodgement machines, arising from a legal requirement that a receipt - including the address - could be issued to customers using this service. The address details were not supposed to be readable by ordinary point-of-sale (POS) terminals found in shops.

Investigation by the institution revealed that some POS terminals had had their software upgraded to a new version, with the unintended result that the address details were read by the terminal and printed on the receipt. Having established the cause of the matter, the financial institution took the following steps:

- Address details were omitted from new Laser cards, in cases where the cardholder did not need to avail of the lodgement facility. In other cases, technical steps were taken to ensure that the address details on new Laser cards could not be printed by POS terminals.
- The Laser cardholders affected by this problem were identified, and a roll-out of replacement Laser cards was initiated.
- The institution took steps to ensure that, whenever the POS terminal software was upgraded in future, it was made aware of this, so that any possible impact on existing Laser cards could be considered.

I considered these steps to be an appropriate response by the financial institution. The important point to emerge from this case is that personal data, stored in debit cards, credit cards, and indeed in any type of card using a magnetic strip or similar storage mechanism, should be kept secure from inappropriate disclosure, in accordance with the requirements of section 2(1)(d) of the Data Protection Act.





Private

Part Three

Guidance

Notes

As Data Protection Commissioner, I recognise that my functions and powers are those which are conferred upon me by law. It is my intention in the years ahead to carry out these duties in full, and to defend the individual's statutory right to privacy, rigorously and firmly. Policy matters are not my main concern, except in the very broadest sense. I will not comment in my annual report on new legislative initiatives, as these are primarily a matter for the Oireachtas, except in very particular circumstances where I feel that clarification of data protection aspects may prove useful.

Of course, it is in my view useful and desirable to give data controllers a clear indication of how data protection law is likely to be applied in practice. This is particularly important given that data protection law is expressed in general terms, and its application in individual cases is not always immediately obvious. Accordingly, in this Annual Report, I include an outline of my thinking on a particular issue - credit referencing - and what I regard as good and acceptable data protection practice for that sector. I also feel it opportune now to comment upon the particular role that data protection has to play in the Reach initiative, which is the driver of e-Government in Ireland.

Guidelines for the Credit Referencing sector

Everyone who applies for a loan from a financial institution is routinely subject to credit referencing, to check their ability to repay the loan, and to facilitate fast, efficient and objective decision-making by the institution. Last year's Report featured an explanation of how the credit referencing system operates in Ireland. This year, I outline the data protection parameters to govern the use of personal data stored on credit referencing databases. While at present there is only one principal credit referencing agency- the Irish Credit Bureau - operating in Ireland, the parameters will apply equally to any other such agency which may become established here in the future. There are four key principles to be observed in a credit reference database, and I will discuss each in turn.

Uniqueness of identification

Entries in a credit referencing database should relate to uniquely identifiable individuals. I do not accept that it is appropriate to maintain records relating to particular households, or to particular family names. Making important decisions or judgements about individuals by drawing inferences from the actions of other persons is not likely to satisfy the "fair processing" requirement of section 2 of the Act.

In order to identify individuals uniquely, and avoid confusion with individuals of similar name and address, financial institutions need to look to section 2(1)(c)(iii) of the Act, which requires that personal data be "adequate" for the particular purpose. This requires that a minimum level of personal data be kept about those who apply for, or have in the past availed of, financial credit. These data would ordinarily need to include full name, full address and date of birth. In addition, section 2(1)(b) of the Act requires that personal data be "accurate and up-to-date". Accordingly, for the financial institution to be in a position to stand over the accuracy and integrity of the personal data, steps should be taken to verify the details supplied by the individual. Reasonable steps regarding identity would, to my mind, include sight of documents such as passport, driver's licence, birth certificate, or other comparable official documentation; and reasonable steps regarding address would include sight of a recent utilities bill.

Where a financial institution has not adhered to these data collection standards, it is not permissible for the credit referencing agency to seek to make good the deficiency by resorting to "close matches", i.e. by associating records relating to distinct individuals living at the same address, or individuals of similar name at distinct addresses. Where ambiguity exists regarding someone's identity - to give a fictional example, whether "B Murphy" of "Cedar Estate, Galway" is the same person as "Bernard Murphy" of "12 Hill View, Cedar Estate, Co. Galway" - I am not inclined to view an association of two such records, which might or might not relate to the same person, as permissible. The onus is on the financial institutions to collect and record personal data in a full and proper manner, and financial institutions must address the consequences of failure in this regard. Indeed, Case Study 4 on page 28 shows the application of this principle in practice.

Openness and Transparency

One of the comments most often addressed to my Office is surprise at the existence of credit referencing database, such as the large database maintained for this purpose in Ireland by the Irish Credit Bureau (ICB). Many individuals seem to be quite unaware that credit referencing is a routine practice - even those individuals who have entered into credit agreements in the past.

I find the lack of public awareness of this important database somewhat worrying, and questions are raised in my mind about the fair obtaining and processing of credit referencing data. Section 2(1)(a) of the Data Protection Act provides that personal data "shall have been obtained, and shall be processed, fairly". Fairness generally involves the informed consent of the data subject, or at the least the apprising of the data subject of the uses to which the data will be put. Traditionally, financial institutions have sought to meet their data protection obligations in this regard by mentioning the credit referencing system among the terms and conditions of a credit agreement. In the future, I will be seeking assurances from financial institutions that individuals are made fully aware, at the time of first entering into a credit agreement, of the use of their data for credit referencing. I am not inclined to regard "small print" as meeting this requirement. It would be preferable, for example, if individuals were required to indicate, in the context of completing the credit agreement contract, that they had read and understood the provisions relating to credit referencing.

Specific to Financial Sector

The members of the ICB are all financial institutions, in the business of providing financial credit to individuals. It would not be acceptable, in my view, if the contents of the ICB credit referencing database were to be disclosed to other types of organisation, not in this particular business. For example, a utility company might normally bill for its product or service on a 30-day arrears basis: however, it could not rely on this billing practice as a basis for accessing the ICB database, to check the credit history of a customer. Such a use of the ICB database would in my view be "incompatible with the purpose" of the ICB database, in contravention of section 2(1)(c)(iii) of the Act. Of course, if the utility company was also in the business of providing financial credit - for example, to enable customers to purchase expensive household items - there would then be no data protection objection to their participation in the credit referencing system, provided that its use of credit referencing information was limited to such purposes.

Use of Personal Data

Once personal data is stored on a credit referencing database, it should be used for bona fide credit referencing only, and not for other purposes. I would make the following points in particular:

- **Lifestyle Profiling:** The credit referencing database should not be used to build up a profile of individuals' spending or borrowing habits, such that groups of individuals could be targeted for direct marketing or approached by financial institutions.

- **Blacklists:** I do not accept that the database, or any part of it, can be used as a "blacklist", such that certain individuals, by their very presence on the list, or by the attachment of certain markers to their record, should automatically be deemed unworthy of credit. The legitimate purpose of the credit referencing database is to provide a point of reference showing a full record of an individual's performance in meeting the terms of credit agreements. Of course, financial institutions are free to exercise their own judgement in deciding whether to do business with an individual, in light of the full facts recorded in his or her credit history.
- **Automated Decision-making:** Related to the previous point, credit referencing agencies should have regard to the provisions of Article 15 of the EU Data Protection Directive, which prohibits automated decision-making procedures in the area of financial credit, without reference to human judgement.
- **Access and disclosure:** A credit referencing agency may record details about those financial institutions that have sought access to a particular individual's credit record in the recent past. This is good practice, as it enables a data subject, who makes an access request to inspect his record, to see which institutions have inspected his or her credit file. It also enables the agency to contact such institutions, in the event of an inaccuracy in the record being discovered, to apprise

them of the corrected information. However, the list of recent enquirers is not part of the credit record, and should not be disclosed as such to other financial institutions. It is not unusual for a prospective borrower to complete application forms with several institutions, in seeking to obtain the most favourable interest rate. There is nothing wrong with this practice and it should have no adverse effect on one's credit rating.

A credit referencing system that meets these criteria is best placed to reconcile the privacy expectations of the public with the legitimate public interest in having an effective and efficient means of assessing creditworthiness.

E-Government and the REACH Project

The Government has recognised the importance of using modern information technologies to deliver public services in better ways. To this end, the Reach agency was established to develop a strategy for delivering e-Government, based on the model of a central "e-broker", holding personal data about citizens in a secure "data vault", with citizens empowered to authorise the transfer of their data to State agencies to facilitate particular transactions. More details about the Reach project can be obtained at the Reach website, www.reach.ie.

I share the view that the e-broker concept is a good model for delivering integrated public services in a manner which is capable of respecting people's privacy and data protection rights. I believe furthermore that it is essential, if the Reach project is to succeed, that respect for people's privacy and for data protection norms be built into the project at design stage. E-Government, if it succeeds in becoming established as a modern, efficient and routine way of dealing with citizens, will do so on the basis of public credibility. Reassurances regarding privacy and respect for the rights of the individual will be needed to counter the long-established fears of an Orwellian "Big Brother", a surveillance society where the State is all-knowing, all-seeing, and traditional ideas of human privacy have been completely displaced by the demands of efficient and unforgiving administration. This is precisely the kind of reassurance that data protection is there to provide, and it is in this sense that data protection is to be seen as an enabler and facilitator of e-Commerce and e-Government alike.

With progress on the Reach project at an advanced stage, and with recent redoubling of e-Government efforts on foot of the "eEurope 2002" Action Plan,

I believe it is timely to re-iterate for everyone some principles of good data protection practice which will inform the development of e-Government in Ireland.

Fair Obtaining of Personal Data

The initial population of the Reach central database with citizens' details is the first issue to be addressed. One approach would be to simply co-opt an existing large-scale database, such as a database of social welfare beneficiaries maintained by the Department of Social, Community and Family Affairs, for this new purpose. This is not an approach I would favour. I believe it is important, in establishing the central database so as to command public confidence from the outset, to respect data protection norms ab initio. Taking personal data that is kept for one purpose, and re-directing the data for a distinct, new purpose without reference to individual's wishes, goes against data protection norms.

The correct approach, I would suggest, involves a process of "re-registering" citizens, giving everyone an opportunity to consent to their inclusion in the new arrangement, and to be informed about the purposes and applications of the central database. Since the Reach initiative is founded upon the principle that the individual citizen is the "owner" of his or her personal data, this principle should be reflected at the initial stage of collecting the data for inclusion in the database.

No Excessive or Irrelevant Personal Data

The items of data to be stored on the central database should be those for which there is a good and valid purpose. Excessive or irrelevant personal data, which are not likely to have a legitimate public service application, should not be asked for or stored.

It seems to me to be sensible to record a "core" of essential, useful personal data in the central database - data such as name, address, Personal Public Service Number (PPSN), and date of birth - and to afford individuals an opportunity, if they wish, to provide additional personal data which has a public service application - e.g. data about health, means, or family circumstances. Individuals who wish to benefit from the potential for improved, more efficient public service can choose to facilitate this by providing a full range of personal data. Individuals who have higher privacy expectations, such as to outweigh the public service benefits, may choose to withhold their personal data, or to provide "core" data only, and instead deal with particular State bodies on a case by case basis in the traditional way. The provision of public services to a citizen should not be contingent upon the citizen's participation in the Reach database.

Use and Disclosure of Personal Data

Individuals should be made fully aware, at data collection or "re-registration" stage, of the range of possible uses of their personal data. In keeping with the concept of their "ownership" of their own data, individuals should be in a position to mandate

or authorise particular uses of personal data within that overall range.

Government Departments and other State bodies that access personal data from the central database should be fully apprised of the authorised uses of the personal data. Uses of data for secondary or other unrelated purposes, without further reference to the wishes of the citizen, should remain subject to the penalties specified under data protection law.

The Reach database will, by its nature, involve disclosure of personal data to a range of State bodies. Naturally, only those items of data that are relevant for a particular transaction should be made available to a State body. The central "e-broker" must ensure that the mandates provided by individual citizens are fully respected, and that no unauthorised uses or disclosures of their personal data can take place. I believe it is necessary and appropriate that the "e-broker" should only facilitate transactions with particular State bodies on the basis of formal and binding agreements.

Combating Fraud

Section 8 of the Data Protection Act, 1988 allows for disclosures of personal data to take place in certain circumstances, to balance the individual's right to privacy against other important public interests. One such circumstance is where the disclosure of personal data is "required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders or assessing or collecting any tax, duty or other moneys owed or payable to the State". This special provision may only be invoked in cases where the normal data protection restrictions on disclosure "would be likely to prejudice" any such investigation, prosecution, assessment etc.

The provisions of section 8 ensure that data protection law is not an obstacle to the tackling of crime and the combat of fraud by the proper authorities. It is quite appropriate, in my view, that these provisions should continue to have full effect in the context of the operations of the "e-broker" and its dealings with State bodies. On the other hand, it would be inappropriate to go further than this, and allow the central database to be used as a universal anti-crime database, or to subject all citizens to automatic screening. The procedures for combating fraud, in the context of the operations of the central database, should be open and transparent, so that they can be seen to be proportionate.

With the above principles enshrined in the Reach project, citizens will, I believe, be able to focus upon the benefits of e-Government, in the assurance that their basic data protection and privacy rights are not endangered. This is by far the most propitious environment for the embedding of e-Government as part of everyday Irish life, and it is one that I as Data Protection Commissioner will do my utmost to support and encourage.

Finally, I should like to add that in my discussions to date with the Reach project personnel, I have found a high appreciation and acceptance of good data protection principles.

Appendices

Appendix One

Receipts and Payments in the year ended 31 December, 2000

1999 £	RECEIPTS	2000 £	€ Euro
342,251	Moneys provided by the Oireachtas (note 1)	340,585	432,454
233,674	Fees	245,203	311,344
-	Legal costs recovered	1,000	1,270
575,925		586,788	745,068
	PAYMENTS		
226,352	Salaries & Allowances (note 2)	242,555	307,981
8,904	Travel & Subsistence	14,977	19,017
27,095	Office & Computer Equipment	7,636	9,696
2,873	Furniture & Fittings	2,574	3,268
11,369	Equipment Maintenance & Office Supplies	5,402	6,859
23,767	Accommodation Costs (Note 3)	7,680	9,752
12,407	Communication Costs	14,259	18,105
4,688	Incidental & Miscellaneous	5,316	6,750
22,408	Education & Awareness	28,220	35,832
2,388	Legal & Professional Fees	4,797	6,091
-	Web Site Construction	7,169	9,103
342,251		340,585	432,454
	Payment of fees and legal refund receipts to Vote for the Office of the Minister for Justice, Equality & Law Reform		
233,674		246,203	312,614
575,925		586,788	745,068

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 these accounts 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 2000 was £53,946 (€68,497); in 1999 it was £50,274 (€63,835).

Appendix Two

REGISTRATIONS 1997 - 2000

	1997	1998	1999	2000
Data controllers by economic sector				
Civil Service Departments/Offices	97	100	106	94
Local Authorities and Vocational Education Committees	118	114	112	111
Health Boards and public hospitals/clinics	42	40	40	55
Third level education	32	33	35	42
Primary and secondary schools	18	19	22	26
Commercial state-sponsored bodies	74	70	72	65
Non-commercial and regulatory public bodies	116	129	139	141
Associated banks	22	25	35	38
Non-associated banks	52	54	51	60
Building societies	8	8	7	7
Insurance and related services	134	137	149	168
Credit Unions and Friendly Societies	451	457	448	448
Credit reference/Debt collection	20	22	23	25
Direct marketing	45	50	54	56
Miscellaneous commercial	19	34	36	65
Private hospitals & clinics/other health	88	92	103	99
Doctors, dentists & other health professionals	269	306	369	386
Pharmacists	515	511	501	491
Political parties & public representatives	84	78	95	96
Religious, voluntary & cultural organisations	40	42	53	51
	2,244	2,321	2,450	2,524
Data Processors	327	329	325	356
Total	2,571	2,650	2,775	2,880





Office of the Data Protection Commissioner

Oifig an Choimisinéara Cosanta Sonraí

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

Bloc 4, An tÁras Árachais,
Sráid Talbóid, Baile Átha Cliath 1

Tel. (01) 874 8544 Fax. (01) 874 5405

Email. info@dataprivacy.ie

Web. www.dataprivacy.ie