



**Data Protection
Commissioner**
An Coimisinéir Cosanta Sonraí

Annual Report 2005

Tuarascáil Bhliantúil 2005

Data Protection at a Glance

What is data protection?

It is the safeguarding of the privacy rights of individuals in relation to the processing of personal data. The Data Protection Acts 1988 and 2003 confer rights on individuals as well as placing responsibilities on those persons processing personal data.

To comply with their data protection obligations data controllers must ...

- obtain and process the information fairly;
- keep it only for one or more specified, explicit and lawful purposes;
- use and disclose it only in ways compatible with these purposes;
- keep it safe and secure;
- keep it accurate, complete and up-to-date;
- ensure that it is adequate, relevant and not excessive;
- retain it no longer than is necessary for the specified purpose or purposes;
- give a copy of his/her personal data to any individual, on request.

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 information about you kept by the organisation;
- stop an organisation from using your details for direct marketing;
- demand that inaccurate information about you be corrected;
- demand that any 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 information about you.

Data Protection Commissioner

Block 6, Irish Life Centre, Lr Abbey Street, Dublin 1

Tel. (01) 874 8544 Fax. (01) 874 5405
LoCall: 1890 252231

eMail. info@dataprotection.ie Web. www.dataprotection.ie

Seventeenth Annual Report

of the Data Protection Commissioner 2005

Presented to each of the Houses of the Oireachtas pursuant to section 14 of the
Data Protection Acts 1988 & 2003.

PRN. A6/0297



What is data protection?

It is the safeguarding of the privacy rights of individuals in relation to the processing of personal data. The Data Protection Acts 1988 and 2003 confer rights on individuals as well as placing responsibilities on those persons processing personal data.





Contents



- 4 Foreword
- 9 Part 1 – Activities in 2005
- 25 Part 2 – Case Studies
- 43 Part 3 – Guidance
- 47 Appendices



Foreword

This is my first report as Data Protection Commissioner. It covers the year 2005 during which my predecessor, Joe Meade, held the post until April.

I gratefully acknowledge the important legacy that has been left by Joe. During his tenure as Commissioner, he significantly advanced the cause of data protection in both the public and private sectors. He also greatly strengthened the standing and operational effectiveness of the Office, something that has put us in a better position to deal with the challenges of decentralisation that face us this year. We are already seeing the many qualities he brought to the post of Commissioner being put into practice in his new and challenging role as the State's first Financial Services Ombudsman.

The Privacy Landscape

At this year's International Conference of Data Protection Commissioners, I was struck by a speaker's remark that 'privacy was in a cold place'. It can certainly appear that way. Privacy – *the right to be let alone* – is being challenged on many fronts.

As part of the so-called 'war on terror', there has been significant curtailment of civil liberties, including the right to privacy, in countries that would traditionally have been viewed as strong supporters of such liberties. States have taken increased powers to acquire information about the private lives of their citizens, often without their knowledge or consent. Such privacy-invasive measures have included the right to demand information from telecommunications companies on an individual's contacts and movements, as revealed by traffic data. International travel increasingly involves intrusive identity checks, including in some cases the compulsory provision of finger-prints – something traditionally confined to those suspected of criminality. There are also moves in some countries that could result in citizens being

obliged to carry State-issued, biometrics-based identity documents and to produce them on demand to police and other State authorities.

There is no doubt about the need for robust measures to protect society against threats to its common welfare. Efficient delivery of State services also calls for measures to make transactions between the citizen and the State easier for both parties. But such measures should be proportionate and acknowledge that the quality of a democratic society is diminished when there is undue intrusion by the State into the individual's 'private space'. I am happy to note increasing evidence that the need for self-restraint by State authorities in these areas is again being recognised.

The other main threat to privacy comes from the commercial sector. In their eagerness to sell their products and services to customers, commercial organisations can sometimes overstep the boundary between legitimate marketing activity and unjustified intrusion into the individual's 'private space'. The worst examples of such excess in the past year have been in the telecommunications sector. There have been some appalling examples of aggressive, privacy-invasive sales tactics being used against vulnerable people. The problems here have been aggravated by the difficulties in putting in place effective measures to give customers their right to 'opt-out' of such direct telemarketing. But I am glad to note that the vast majority of companies are eager to respect the individual's right to privacy, recognising that virtue in this area brings its own commercial rewards in terms of customer trust and loyalty. I am also hopeful that the problems with the effective operation of the telemarketing 'opt-out' - the right under law not to receive marketing calls - will be resolved shortly.

There is no doubt about the need for robust measures to protect society against threats to its common welfare

It is clear that privacy matters to Irish people. A survey commissioned by my office towards the end of 2005 revealed that it came second only to crime in its relative importance to individuals. This result is not entirely surprising, given the staunchly independent streak in the Irish character and a related reserve in terms of ceding power to the State.

The survey also showed that there is concern amongst Irish people about using the internet in terms of disclosing credit card details and the possibility of internet fraud. Similarly, there are low levels of trust in conducting business with companies on the internet, even well known companies. The survey results also showed that, while awareness of data protection has increased since the last survey in 2002, younger (18-24 year olds) and older people (50+), and those from lower socio economic groups, display lowest levels of awareness, knowledge and perceived importance of personal privacy issues. I intend to focus awareness initiatives on these groups in the future in order to reduce their exposure to data privacy risks, and raise overall awareness of the Data Protection Commissioner's office.

Persuasion and Dissuasion

Data protection law exists to protect our personal information from being used or disclosed to third parties for purposes other than those for which we provided the data. It is a complex body of law which is contained mainly in the Data Protection Acts 1988 and 2003 and in the European Communities (Electronic Communications Networks and Services)(Data Protection and Privacy) Regulations 2003 (S.I. No.535 of 2003).

Emanating from the EU Data Protection Directive 95/46/EC and the Council of Europe Data Protection Convention 108 of 1981, the Acts recognise that the protection of privacy in regard to personal data are a human right. The right to privacy has been recognised by the Irish Courts as one of the fundamental personal rights of the citizen. The right to privacy is explicitly provided for in Article 8 of the European Convention on Human Rights.

My aim is to make data protection law relevant, easy to understand and pragmatic. It is not there to stop organisations doing their legitimate business. Rather, it provides a framework for good data handling practices which should balance organisational requirements with the individual's right to privacy.

The Office of the Data Protection Commissioner is part of the State's family of human rights agencies. The particular right we help to uphold is the right to privacy.

My functions under the Data Protection Acts and related legislation fall into 3 main categories:

- **Ombudsman Role:** resolution of disputes between individuals and data controllers or processors
- **Enforcer Role:** compliance by data controllers and processors
- **Educational Role:** Promoting data protection rights and good practice

In my ombudsman role, my focus is on achieving mediated solutions, where possible. Complaints offer a useful insight into the concerns of people, helping to guide the educational activities of the Office.

In the Office's experience, most 'data controllers' – those who hold personal information on individuals – recognise the need to respect the privacy of individuals. Data protection legislation is based on certain core principles (summarised on the inside cover of this report) and gives a wide degree of discretion as to how these principles should be applied in particular circumstances. Generally, breaches of data protection legislation are unintentional and the majority of data controllers are happy to correct any practices that contravene our legislation.

For the majority of compliant data controllers, my approach is one of helping them to achieve better respect for privacy by offering targeted guidance. For the minority who wilfully or carelessly infringe people's privacy rights, my approach is to use the full extent of my powers to achieve quick correction of such behaviour.

The educational role of the Office is a broad one. It encompasses everything from public information campaigns, to targeted advice to particular companies, to private discussions with Government agencies on new legislative proposals.

Educating people on their right to data privacy is important. Only if people know their rights can they take effective measures to vindicate them. My objective is that, through greater awareness of data protection rights, people will be empowered to protect their own privacy. The Office's work with different sectoral groups – especially activities with a 'multiplier' effect – is a critical part of our mission.

Trying to build privacy protection into policy proposals at an early stage is another vital part of the Office's work. In our experience, working with government agencies and commercial bodies at an early stage means that privacy protection can be part of the solution and not - as it is sometimes presented - a barrier to progress. I intend to give particular emphasis to this aspect of our work.

During the past year, the Office was consulted on such issues as : the proposed Public Service Card; Health records and a unique identifier for Health; Biometrics in Passports, and Genetic Data. Our approach in all cases has been to focus on minimising the intrusion on the individual's privacy and maximise transparency.

Developing Standards through Codes of Practice

Personal data are, of course, a business asset and I have no wish to restrict businesses in their work or to impose unnecessary regulatory burdens. I will be seeking to develop a standards-based approach to data protection across the public, private and voluntary sectors. I will be encouraging sectoral bodies to develop Codes of Practice which will tailor the data protection principles to the particular conditions applying in that sector. Under section 13 of the Acts, such a Code approved by me, may be laid by the Minister before each House of the Oireachtas and, if approved by resolution, has the force of Law.

A welcome development during the year was the publication by the Department of Justice, Equality and Law Reform of a Code of Practice for community CCTV schemes. I was also happy to see progress being made on the development of a Code of Practice for data protection in An Garda Síochána. I would welcome greater effort on the part of the private sector to develop such codes.

Data Protection and the Media

During the year, my Office received three complaints from individuals alleging that their data protection rights had been contravened by media publication. In my opinion, the effect of the section 22A Data Protection Act media exemption is that publication of personal data are only to be permitted where the 'journalistic purposes' outweigh the data subject's

right to privacy, to the extent that non-publication would seriously breach the public's interest in freedom of expression. I fully accept the importance of the right of freedom of expression and recognise that the public interest in maintaining a free press and media must be defended. However, I consider that there are limits to what the Press may publish when this could cut across data protection rights and I deal with this in some detail in Part 1. I believe that data protection law may have a modest contribution to make to the achievement of a balanced outcome to the current national debate on defamation and privacy.

'Cold Calling'

One of the greatest sources of complaint to the Office during the year was from individuals who had been pestered in their homes by telecommunications companies seeking to persuade them to change from their existing telecommunications provider. Complainants spoke of aggressive and repeated calls, often from outside the State.

The public attitudes survey which we commissioned last year showed strong opposition to 'cold calling' to domestic phone lines. This, and the pattern of complaints we received, makes me particularly determined to clamp down on abusive direct marketing. The right of customers to 'opt-out' of receiving such calls is not yet operating satisfactorily. Working with ComReg, I hope that this situation will be resolved in the course of the coming year.

I welcome the decision by the Financial Regulator to completely ban such 'cold-calling' in relation to financial services, as part of its Customer Code. The case for extending this approach to other sectors is strengthened by the abuses that have come to light during the year and the unsatisfactory operation of the 'opt-out' regime.

Data Protection and An Garda Síochána

Data protection can pose particular challenges for police forces. The rights of individuals – including their right to data privacy – must be balanced against the need to protect the community through effective enforcement of the law. The Data Protection Acts recognise this, by providing for wide exemptions where the security of the State or criminal investigations are involved. However, the use of such exemptions must be justified on a case-by-case basis. This applies particularly in relation to an individual's right to access personal data held on her/him by An Garda Síochána.

My Office has been working closely with An Garda Síochána in helping to improve understanding of data protection principles at all levels of the force. Garda management responded positively to the recommendations of an audit conducted in 2004 on aspects of data protection. I look forward to early implementation of one of the key recommendations of that audit; the production of a data protection Code of Practice for An Garda Síochána. I believe that the Code will help overcome some of the difficulties that have been experienced in this area, notably delays in responding to requests by individuals for copies of personal data held on them by An Garda Síochána.

Decentralisation

During the year, planning for the Office's decentralisation to Portllington was stepped up. The Office's revised Implementation Plan was published in November 2005 and was predicated on the actual move to new premises in Portllington taking place in Autumn 2007. It now appears likely that the move will be brought forward to later this year. All but one of the staff have indicated that they will not transfer with the Office, so the coming year will be one of transition, as new staff arrive through the Central Applications Facility (CAF) process and on promotion. As part of the preparatory process for the move, work

has been stepped-up on up-grading our records management and on mapping our work processes. The Office's website, www.dataprotection.ie, was substantially upgraded, including the publication of comprehensive new guidance.

Outlook for 2006 and beyond

In the midst of this staff turnover, the forthcoming year will be a challenging one as we seek to maintain service levels in relation to our statutory functions.

Privacy is a somewhat nebulous concept, the absence of which is often noticed only after there has been a breach. Results from the 2005 survey confirm that maintaining privacy in relation to personal information and use of the Internet, and opposition to receiving unsolicited direct marketing, are areas of concern to Irish people. Technology will continue to pose challenges to privacy, while also offering solutions through Privacy Enhancing Technologies (PETs). The threat of further State encroachment on personal privacy will probably be an increasing challenge. But our experience since the passing of the Data Protection Act 1988 suggests strongly that respect for data protection principles need not be a barrier to more efficient delivery of services from either the public or private sectors.

Data protection is fundamentally about recognising the individual's right to determine how personal information about her or him is used. Such respect for an individual's 'private space' should be seen as one of the foundations of a civilised and democratic society.

Appreciation

I thank the many people who contacted my Office and brought serious matters to attention or who simply called for advice on how to achieve best practice in their organisation. Most data controllers generally complied fully with the law and I am grateful for their co-operative approach.

I wish to thank the Minister for Justice, Equality and Law Reform and his officials for their support and to express my commitment to fostering the good relations between our Offices.

Finally I want to thank my Office staff for their commitment and dedication to the objectives of data protection, at a time when, for most of them, this will be their last year dealing with data protection issues. Their commitment in this difficult time of transition to decentralisation is in the best traditions of the public service. I commend them for it.



Billy Hawkes
Data Protection Commissioner

3 March 2006

Part 1 - Activities in 2005

10	Introduction	18	The Media
10	Business Planning Review	20	Garda matters
11	Promoting Awareness	20	The Public Register
12	Customer Service and Provision of Information and Advice	20	Privacy Audits
13	Information for Data Subjects	21	International Activities
13	Privacy and Telecommunications	22	European Activities
15	Complaints and Investigations	23	Transborder Data Flows
18	Prosecution	23	Administration

Introduction

The Data Protection Acts 1988 and 2003 create a framework for the handling of personal data across all sectors of society - public, private and voluntary. Personal data are a somewhat nebulous concept - it refers to data about each of us as individuals, from the most innocuous to the most sensitive, such as our health or genetic data. Organisations processing personal data are obliged to protect these data, individuals who are the subject of contraventions may cite the Acts in suing for damages and I, as Commissioner, can take enforcement action, up to and including prosecutions, depending on the circumstances.

Although the Data Protection Acts create legal rights and obligations, it is not my intention to take an overly legalistic approach to enforcement in this area. Rather, I want to encourage the pragmatic application of the law with the overall goal of ensuring that peoples' personal data are protected. The main principles which the Acts express, and which are reproduced on the inside cover of this Report, are readily understandable. They make good business sense for all organisations – treat peoples' data, especially their sensitive personal data (health data for example) with respect, obtain it fairly, do not seek excessive information, use it only for the purposes intended, do not disclose it and keep it secure.

These simple rules ought to be easy to follow and to an extent are common sense. They must be respected by every organisation or otherwise people will be reluctant to trust the developing e-government and e-commerce channels. **My aim for data protection is to make these rules and their relevance widely understood and for my Office to be an enabler and facilitator of good data protection and an effective enforcer where serious abuses occur.**

In the following pages, I seek to give a snapshot of the work of the Office in 2005.

Business Planning review

In November 2005, Office staff participated in a review of our Business Objectives which culminated in the finalisation of our Strategy Statement and Business Plan for 2006 which is published on our website. One of the principal factors affecting the Business Plan in 2006 and the delivery of our objectives is the impact of preparing for decentralisation of the Office to Portllington. This is now likely to take place later this year, a year earlier than anticipated when the Business Plan and associated revised Decentralisation Plan were drawn up. During 2006, it is anticipated that there will be an almost 100 per cent turnover of staff. We are taking all possible steps to mitigate the risks to business continuity that will arise from this. We are focussing in particular on measures to retain our corporate memory – especially by putting the maximum amount of useful guidance on our website.

I regard the promotion of public awareness of Data Protection as one of the most important functions of the Office

Promoting Public Awareness

I regard the promotion of public awareness of Data Protection as one of the most important functions of the Office. During the year, the following education and awareness initiatives were undertaken:

- Completed production of and launch of a specially commissioned training video and accompanying facilitators handbook. The video, which is available in CD and DVD format, is based around the Eight Data Protection Rules and portrays the operations of a company and how inattention to data protection can damage the business. The aim of the video is to provide a resource for data controllers in training their staff on the core data protection principles. I am pleased to record that over 160 copies of the video have been requested by and distributed to data controllers and the feedback has been very positive.
- Continued participation in The Graduate Treasure Trail Quiz, an online competition for primary and secondary school students.
- Commissioned a nationwide radio advertisement campaign to promote the launch of the telemarketing opt-out on the National Directory Database in July.

- Re-ran a nationwide public awareness poster campaign on buses and trains in October.
- Commissioned a public awareness survey, which was a comparative follow-up to a 2002 survey.
- Made some 37 presentations to groups in the public, private and voluntary sectors.
- Contributed to the broadcast and print media, as data protection issues arose.

The results from the 2005 survey indicate that people are increasingly concerned at maintaining privacy in relation to personal information, especially when using the Internet. They also express opposition to receiving unsolicited direct marketing. Some key pointers from the survey are that:

- Privacy of personal information continues to be of utmost importance to Irish people with almost nine out of ten claiming it to be very important to them personally.

- Financial history achieves greatest levels of importance (almost 9 out of 10 – very important). However medical records, credit card details and Personal Public Service Number (PPSN) is mentioned by 8 of 10 respondents. Interestingly this year, the PPSN has grown in importance in terms of keeping it private compared to previous years (84 % very important in 2005 vs.60% in 2002).
- There is concern amongst Irish people about using the internet in terms of disclosing credit card details and the possibility of internet fraud. Similarly there are low levels of trust in dealing with companies on the internet, even well known companies.
- People continue to be opposed to receiving unsolicited direct marketing, particularly to their home phones.
- Consistently across all measures, younger (18-24 year olds) and older people (50+), and those from lower socio economic groups display lowest levels of awareness, knowledge and perceived importance of personal privacy issues.
- Currently one in two Irish people are aware of the Data Protection Commissioner compared to two in five in 2002. In addition, the proportion of people who would complain to the Data Protection Commissioner's office about invasion of privacy has increased significantly since 2002 and 1997 (2005-18%; 2002 8% and 1997 2%).
- While the recent advertising campaign was effective in terms of being seen by one in four adults, particularly those who are aware of the Data Protection Commissioner (almost one in two), it impacted more on 25-49 year olds and ABC1's than younger and older age groups and C2DE's.

I welcome the encouraging nature of these results and it is my intention to focus our education and awareness activities in 2006 in the light of them.

Customer Service and the Provision of Information and Advice

As a public office customer service is paramount. The Office has published on the website (www.dataprotection.ie) a revised Customer Charter and Action Plan. These documents set out detailed Customer Service targets, key performance indicators and outline how we intend to monitor our performance against our targets.

The Office is very focussed on the provision of comprehensive and practical advice on data protection. Indeed much of the day-to-day work of the Office entails the provision of advice and information in response to enquiries received either in person, by phone, email or post. In 2005 the Office dealt with in excess of 15,000 enquiries by phone and an ever increasing number of enquires by email, over 1,000 in 2005. Our callers include business, public bodies, members of the public as well as people who may be advising others (legal professionals, educators, citizens advice centres). Our public awareness initiatives which were aimed at making the general public more aware of their rights, have also resulted in generating more requests for advice.

We have found that a valuable source of information is our website (www.dataprotection.ie) and during the year, my Office engaged in a complete revamp of the website. It was relaunched in the Spring with new and more detailed Guidance and incorporating a search engine. It also complies fully with the Web Accessibility Initiative guidelines level AA for public websites, the primary goal of these guidelines being to make web content accessible to people with disabilities.

During the year, 37 presentations were made by staff of the Office and myself to various sectors and

organisations. These were well received generally and serve the dual function of bringing the Office into face to face contact with data controllers on the ground and of communicating what this Office expects in terms of compliance with data protection obligations. Details of presentations given are in Appendix 1.

Information for Data Subjects

One of the most important features of the Acts is the right to be made aware, pursuant to section 2D, of the identity of the data controller, the purposes of processing, to whom the data has been or will be disclosed and any other information which is necessary in order for the processing to be fair to the data subject.

As regards fairness, a matter which has come to my attention recently is the impression held by a small number of data controllers that, if they get a data subject's prior consent, then it is in order to require that person to agree to the collection or disclosure of their personal data in ways incompatible with data protection law. For instance, one insurance company sought to have applicants for their products sign a general consent agreement enabling the Company to have credit checks carried out on them before renewing their annual insurance policy. In this regard, I would like to point out that data protection principles require that any personal information processed must be adequate, relevant and not excessive in relation to the purposes for which the information is collected, and it is not compatible with data protection law to require data subjects to consent to setting aside their statutory entitlements to data protection.

Privacy and Telecommunications

There were a number of developments in this sector during the year. Principal amongst them were the

launching of the NDD opt-out facility and the first prosecution for 'SPAM'.

The NDD launch

The National Directory Database (NDD) has traditionally existed as a resource that is used to provide information for directory enquiry searches and for publishing telephone directories. EU Directive 97/66/EC (concerning the processing of personal data and the protection of privacy in the telecommunications sector) introduced the right for telephone subscribers to object to receiving unsolicited telecommunications for the purpose of direct marketing, more commonly referred to as 'cold calls'. Statutory Instrument 192 of 2002 (later replaced by SI 535/2003) transposed this into Irish law. In order to facilitate this right to object, it was decided to allow the recording of opt-outs on an existing central database of phone numbers, the NDD. Following prolonged discussion with industry, this facility was officially launched on 21 July 2005.

A person who does not wish to receive marketing phone calls now has a right to contact the person to whom they pay telephone line rental and have their preference not to receive marketing calls recorded on the NDD. If they receive marketing calls 28 days after their preference has been recorded on the NDD, the caller has committed an offence and may be prosecuted by my Office.

Initial problems with the launch of the NDD.

Although all telecommunications service providers had been given adequate notice of this new facility, I was disappointed that two of the main service providers experienced difficulties in ensuring that their own subscribers' requests were properly recorded on the NDD. EsatBT experienced short term difficulties that resulted in some delay to the recording of preferences on the NDD. However, Eircom experienced a number of difficulties in operating the system. This resulted in

an uncertain number of initial requests being lost and took a number of months to resolve. This was disappointing considering the fact that Eircom hosts the NDD and therefore should have reasonably been expected to be in a better position to operate the system than others. Given the difficulties experienced, in cooperation with the Commission for Communication Regulation (ComReg), I instructed Eircom to directly notify all customers who may have been affected by the problems it had experienced in order that they might express their preference again.

Ex-directory telephone numbers.

The choice of the NDD as the central facility for recording opt-outs has resulted in one problem; the NDD does not record details of ex-directory subscribers. This resulted in ex-directory subscribers being unable to avail of the protection offered by the NDD. I found this to be a totally absurd and unacceptable position and initiated enforcement action in December 2005 to ensure that ex-directory subscribers would be able to have their preferences respected. Currently, my office is in discussion with ComReg, Eircom (as NDD host) and all telecommunications service providers to progress the matter. Although at an early stage, initial discussion has been favourable.

Co-operation with ComReg and RegTel

Although I have been given certain responsibilities under SI 535 of 2003, in many cases these are shared with ComReg and consultation is a requirement. I enjoy a close and productive working relationship with ComReg, including regular meetings between myself and Commissioner Mike Byrne. The assistance of ComReg staff has been of great value to my Office. The Regulator of Premium Rate Telecommunications Services (RegTel) also continues to provide valuable assistance in investigations.

Enforcement and compliance

September 2005 saw the first prosecution under Regulation 13 of SI 535/2003 (See case study 11). This prosecution attracted a high level of media attention and it is noticeable that there has been a significant decline in complaints of a similar nature. This may indicate that the industry has taken note both of its responsibilities and my willingness to take appropriate enforcement action. But whilst one sector appears to have tidied itself up, the same cannot be said for others. In particular, some providers of telecommunications services appear to have a casual interest in data protection. Most cold calling complaints made to this office relate to the operation of telecommunication service providers, with two companies (Optic Communications and NewTel Communications) standing out. Given that telecommunication service providers have special obligations under SI 535 of 2003 and have had significant contact with this Office concerning the operation of the NDD, I find it difficult to understand how people in that industry can appear to ignore their legal obligations.

Investigations into a number of these companies revolved around their persistent failure to respect opt-outs expressed by people whom they had called. I was not surprised to discover that some complainants had reported callers to An Garda Síochána on the basis of the offensive or threatening content of calls. The nature of complaints made to my Office certainly indicated bizarre activity. Investigations involving a number of companies are now at an advanced stage and prosecutions are being actively considered.

Communications Traffic Data Retention

Part VII of the Criminal Justice (Terrorist Offences) Act 2005 provides for the compulsory retention of telephone traffic data by telecommunications operators for 3 years and for such data to be made available to the Garda Síochána on request. The background to this development is given in last year's

Under the Data Protection Acts, 1988 & 2003, I may launch an investigation into the possible contravention of the Acts where an individual complains to me that their data protection rights may have been infringed in any way...

Report. At the end of the year, the European Council and Parliament agreed the text of a Directive providing for a uniform system of communications traffic data retention throughout the EU.

Transposition of the Directive into Irish law will offer an opportunity to review the provisions of the 2005 Act. From a data protection perspective, it would be helpful if the revised Irish legislation limited the right of Garda access to cases of serious crime and if the safeguards against potential abuse of such access rights were strengthened.

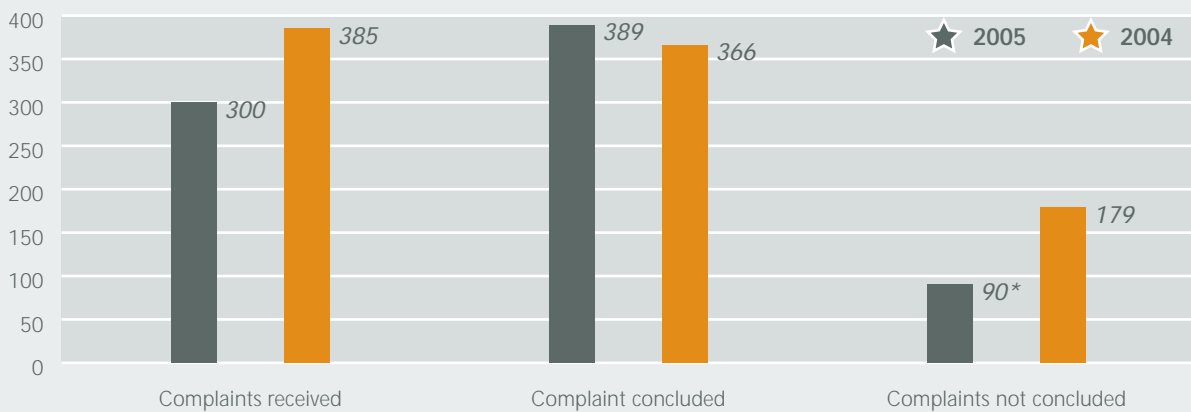
Complaints and Investigations

Under the Data Protection Acts, 1988 & 2003, I may launch an investigation into the possible contravention of the Acts where an individual complains to me that their data protection rights may have been infringed in any way, or where I am of the opinion that there may be a contravention. Where a complaint is received, I, as Commissioner, am required by section 10 of the Acts, to investigate it, and, to try to arrange an amicable resolution. Failing that, I am required to issue a decision in relation to it. As in previous years, my Office managed to resolve the greater proportion of complaints informally, without it being necessary for me to issue a formal decision under section 10.

I regard the complaints and investigations function as being of central importance in my Office. Addressing alleged contraventions of the Acts in a proactive manner means that individuals can see that upholding their data protection rights is taken seriously by my Office, while organisations where a contravention has been established, are required to address shortcomings and put new procedures and practices in place. I do not hesitate, where necessary, to issue Enforcement Notices requiring data controllers to desist from practices that breach the Acts. Where I find that there has been a breach of the Acts, individuals may use my decision to support a claim for damages in the courts under section 7 of the Acts.

During 2005, as in previous years, the increasing complexity of the case-load posed challenges for the staff. The number of new complaints received during the year was 300 compared to 385 in 2004. The biggest factor in this decrease was the significant reduction in the number of complaints dealt with under the Privacy in Electronic Communications Regulations (S. I. No.535 of 2003), 66 in 2005 compared to 131 in 2004. The number of complaints concluded during 2005 was 389 and at the end of the year 90 were still on hand. This is illustrated in **Figure 1**.

Figure 1 Complaints received, concluded and not concluded



* 90 Complaints not concluded at 31 December comprised of: on going inquiry 5, with the data subject 3, with the data controller 65, with the Office for review and further consideration 17

Figure 2 shows a breakdown of the types of organisation against which complaints were made in 2005. 15 % of complaints concerned the direct marketing sector. The telecommunications/IT sectors accounted for 20 %, while the financial services sector accounted for 18% of complaints. The public

services and Central Government accounted for 20% of complaints.

As regards the grounds for complaint, see Figure 3, the largest areas of complaint concerned the exercise of the right of access to data under section 4 of the

Figure 2 Breakdown of data controllers by sector

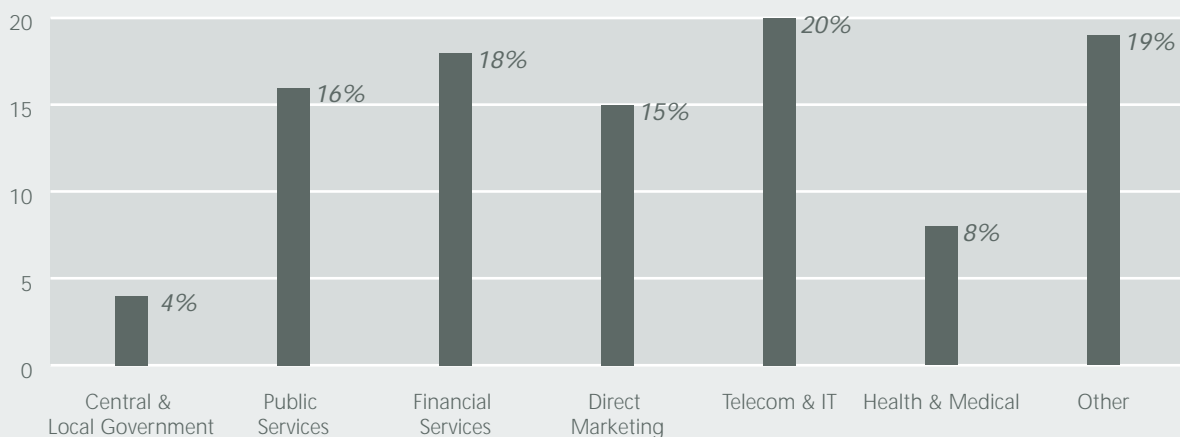
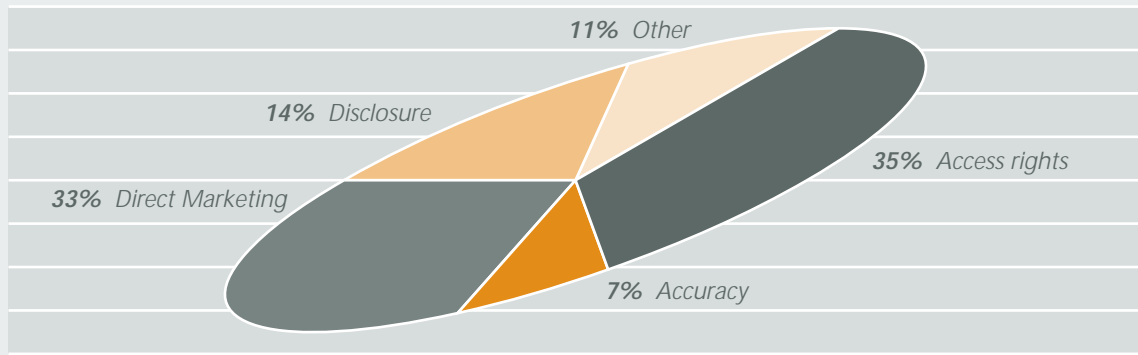


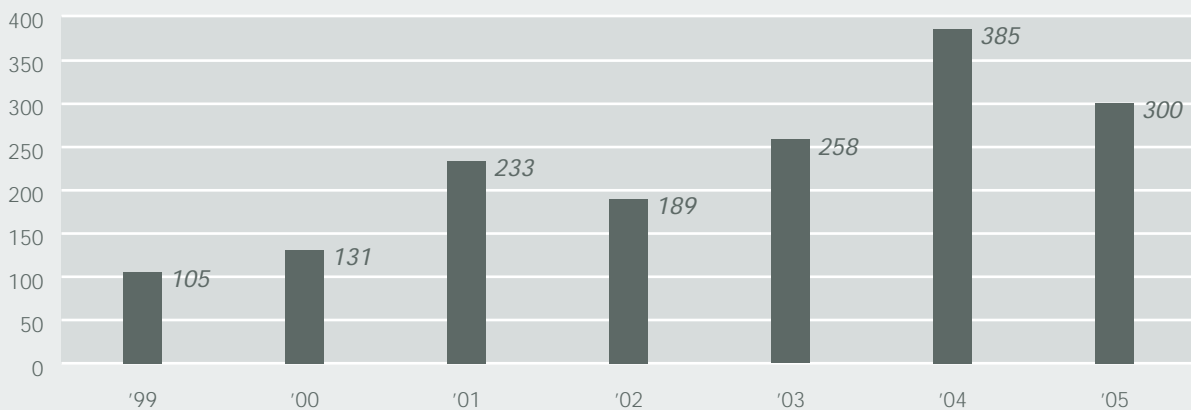
Figure 3 Breakdown of complaints by data protection issue



Acts (35%) and complaints in relation to direct marketing, including telemarketing (33%). Complaints about the issue of fair obtaining and incompatible disclosures of data to third parties were the next most common issue of complaint (together totalling 15%).

Of the complaints concluded, 45% were resolved informally, 27% were upheld and 28% were rejected. Details of the more significant cases are summarised in the Case Studies section of this Report.

Figure 4 Complaints received since 1999



Prosecution

During 2005, I took my first prosecution for an offence under Regulation 13 of Statutory Instrument 535 of 2003. 4's A Fortune Limited was convicted in the District Court on five counts of contravening Regulation 13(1)(b), in that it sent marketing messages to five mobile phones without the consent of the subscribers.

The Company faced a potential fine of up to €3,000 per message sent, and was fined €300 per count by the Court (a total of €1,500). The Company was also ordered to pay costs of €1,000. I am satisfied that this case has sent out a positive signal to the marketing community and to those that are targets of its promotions. Although prosecution is not an option undertaken lightly, I am not reluctant to pursue this route when necessary.

Since investigation of this case commenced, complaints about similar promotions have fallen and I believe that this is, in part, due to the marketing sector taking proper notice of their legal obligations and acting in a lawful manner.

The Media

During the year, I received three complaints from data subjects alleging that their data protection rights had been breached by publication of material about them in the media.

Section 22A (1) of the Acts provides an exemption from the requirements to comply with the fair obtaining and legitimate processing requirements of sections 2, 2A(1) and 2B(1) of the Acts. It provides as follows:

"22A(1) Personal data that are processed only for journalistic, artistic or literary purposes shall be exempt from compliance with any provisions of this Act specified in subsection (2) of this section if-

- (a) the processing is undertaken solely with a view to the publication of any journalistic, literary or artistic material,*
- (b) the data controller reasonably believes that, having regard in particular to the special importance of the public interest in freedom of expression, such publication would be in the public interest, and*
- (c) the data controller reasonably believes that, in all the circumstances, compliance with that provision would be incompatible with journalistic, artistic or literary purposes".*

While this section refers to the 'reasonable belief' of the data controller, it does not, in my opinion, give a newspaper editor the sole discretion to judge if something is in the public interest. This point is perhaps more clearly expressed in Article 9 of the Data Protection Directive (95/46/EC) on which section 22A is based. This states that " *Member States shall provide for exemptions or derogations from the provisions of (the Directive) for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression. "*

In the case of a complaint received by me, I must therefore judge if the data controller properly balanced the right to privacy with the public interest in disclosure. I must have regard to the nature of the facts, including whether the data relates to a public figure or a relative of a public figure, the age of the data subject and whether sensitive data within the meaning of the Acts is involved.

In this respect, the Decision of the European Court of Human Rights in the case of Von Hannover v. Germany (Application No. 59320/00) - the Princess Caroline case - is relevant. In this case, the Court held that the German courts, in refusing to grant Princess Caroline of Monaco injunctions against newspapers taking and publishing photographs of her, had infringed her

rights under Article 8 of the Convention (which deals with the right to privacy). The photographs in question had shown Princess Caroline engaged in various activities, associated with no official functions, such as shopping, practising sport and lying on a beach. The Court said -

"64. ...although the public has a right to be informed, which is an essential right in a democratic society that, in certain special circumstances, can even extend to aspects of the private life of public figures, particularly where politicians are concerned, this is not the case here. The situation here does not come within the sphere of any political or public debate because the published photos and accompanying commentaries relate exclusively to details of the applicant's private life.

65. As in other similar cases it has examined, the Court considers that the publication of the photos and articles in question, of which the sole purpose was to satisfy the curiosity of a particular readership regarding the details of the applicant's private life, cannot be deemed to contribute to any debate of general interest to society despite the applicant being known to the public.

66. In these circumstances, freedom of expression calls for a narrower interpretation...

69. The Court re-iterates the fundamental importance of protecting private life from the point of view of the development of every human being's personality. That protection - as stated above - extends beyond the private family circle and also includes a social dimension. The Court considers that anyone, even if they are known to the general public, must be able to enjoy a 'legitimate expectation' of protection and of respect for their private life."

While data protection was not dealt with directly in the Decision, this case is of assistance in helping me to weigh the balance between the public interest and freedom of expression as required by section 22A of the Acts. In my opinion, the effect of section 22A is that publication of sensitive personal data will only be

permitted where the 'journalistic purposes' arising outweigh the data subject's right to privacy, to the extent that non-publication would breach the public's interest in freedom of expression. I fully accept the importance of the right of freedom of expression and recognise that the public interest in maintaining a free press and media must not be unduly compromised.

In assessing the balance in this matter, I note the National Newspapers of Ireland Code of Practice on Privacy (1 July 1997) which in section 10 reads as follows:

"Children should not be identified unless there is a clear public interest in doing so. Relevant factors include what age the child is, whether there is parental permission if the child is too young to consent and what are the circumstances, if any, that make the story one of public interest, or if the person is a public figure or child of a public figure, whether or how the matter relates to his/her public person or office.

Note: For the purpose of this code, the public interest may be defined as:

- (i) Detecting or opposing crime or a serious misdemeanour***
- (ii) Protecting public health and safety***
- (iii) Preventing the public from being misled by some statement or action of an individual or organisation.***

When raising issues beyond these three, it is for the editor of the publication involved to demonstrate how the public interest would be served."

I consider that these guidelines are a fair expression of how the principles of data protection legislation ought to be applied in practice. In the 2003 Annual Report (page 18), my predecessor placed emphasis on the importance of parental consent and the protection of minors in the context of publication of photos of young people by a voluntary organisation.

Accordingly, in matters involving children under 16, editors should demonstrate the existence of an exceptional public interest in order to over-ride the normally paramount interest of the child.

Garda matters

During the year, the issue of subject access to personal data held by An Garda Síochána arose. The Office's clear position, which has been communicated to the Garda authorities on many occasions in recent years, is that the Gardaí can claim the application of section 5(1)(a) of the Acts to relevant data, even in circumstances where an investigation has been finalised. However, in so claiming they must have regard to the prejudice test in respect of each item of data. Section 5(1) of the Acts provides as follows:

"Section 4 of this Act does not apply to personal data:

(a) kept for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders or assessing or collecting any tax, duty or other moneys owed or payable to the State, a local authority or a health board, in any case in which the application of that section to the data would be likely to prejudice any of the matters aforesaid,"

It is clear that this exemption is only available where compliance with section 4 would be likely to prejudice the preventing, detecting or investigating of offences, or apprehending or prosecuting offenders. It is not a general exemption and every time it is claimed in respect of particular data, it has to be on a case by case basis. This involves the data controller, in this case An Garda Síochána, exercising its judgement based on the particular circumstances of the case. My view is that 'likely to prejudice' requires a significant likelihood rather than a mere risk that the purposes set out in section 5(1) would be noticeably prejudiced if the individual were to have access to the personal data held about him/her. This implies that the Gardaí cannot withhold access to all information held about an individual, only that information which relates to the objectives set out in section 5(1).

I am satisfied that the Garda authorities take their responsibilities under the Data Protection Acts seriously. The difficulties that have been experienced in this area should be greatly reduced when the Garda Data Protection Code is finalised, probably later this year.

The Public Register

In 2005 the number of organisations registered increased by 424 or 8% (see Appendix 2). Schools, insurance related services and health professionals were the main sectors accounting for the increase.

As the consultation process within the Department of Justice, Equality and Law Reform into the requirement to register was ongoing, I decided not to pursue any specific sectors in relation to their registration requirement during the course of 2005. I look forward to new Regulations on registration being signed by the Minister in the course of 2006, following the anticipated commencement of the new section 16 of the Data Protection Acts.

My office has been looking at the feasibility of implementing an on-line payments system where organisations can pay their annual registration fee via our website www.dataprotection.ie. It is hoped that this will be in place during the first half of 2006.

Privacy audits

The Data Protection Amendment Act 2003 gave the Office a more proactive role. My powers to enforce the Acts were strengthened and clarified. In particular, I now have the power to carry out investigations as I see fit, in order to ensure compliance with the Acts and to identify possible breaches. This power can be used to conduct comprehensive privacy audits of data controllers. Such audits are supplementary to investigations carried out in response to specific complaints.

In the course of 2005, 3 comprehensive audits were carried out. Those audited in 2005 were: The Irish Credit Bureau, Tesco Ireland Ltd and Lucan District Credit Union Ltd.

As in 2004, I am happy to report that my inspection teams found that there is a reasonably good awareness of and compliance with the data protection principles in the organisations that were inspected. A number of recommendations were made in each case. I am pleased to report that the data controllers concerned were willing to put procedures in place to ensure that they were fully compliant with their data protection responsibilities. I would like to thank the three organisations for their cooperation.

I regret that resource constraints did not permit us to carry out more audits, as I believe they are a very valuable tool for improving compliance with data protection principles. Despite the challenges of decentralisation, I hope to increase the number of audits conducted in the course of 2006.

International Activities

During 2005 my staff and I participated in the following international activities -

- *Article 29 Working Party of the EU Data Protection Commissioners, the EU Data Protection Supervisor and the EU Commission.*
- *EU Joint Supervisory Bodies comprising Europol, Schengen, Customs Information System, Eurodac and Eurojust as well as the related Appeals Committees.*
- *27th Annual International Conference of Privacy and Data Protection Commissioners in Montreux, Switzerland.*
- *Spring Conference of European Data Protection Commissioners in Krakow, Poland.*
- *International Complaints Handling Workshops in Budapest and Paris.*

- *International Working Group on Data Protection in Telecommunications in Portugal.*
- *Annual meeting of the United Kingdom, Irish, Guernsey, Jersey, Cyprus, Malta and the Isle of Man authorities in Cyprus.*
- *Meetings in Manchester with the United Kingdom Information Commissioner and in Dublin and Belfast with the Assistant Commissioner with responsibility for Northern Ireland matters.*

The International Conference of Privacy and Data Protection Commissioners in Montreux, Switzerland brought into focus the international dimension to Data Protection and underlined that furtherance of the Data Protection agenda depends on co-operation at the international level and with industry. There was a sense amongst delegates that protecting the individual's right to privacy was becoming increasingly difficult, due both to privacy-invasive technologies (the Web etc) and the actions of Government in relation to security. While Data Protection Authorities needed to recognise this reality, their public duty is to uphold the human right to personal data protection and it was felt that action could most effectively be taken in the following areas:

- Working with the IT sector to build Privacy Enhancing Technologies (PETs) into IT applications and encourage progression towards universal standards
- Recognising the legitimacy of governments' security concerns in the face of terrorist threats and working with them on solutions that achieved security objectives without unnecessarily compromising privacy.
- Privacy Impact Assessments were needed on legislative proposals generally (PIA's)
- Recognising and building on new consumer-driven privacy-enhancing legislation (e.g. California's security breach legislation, obliging companies to inform customers when the security of their data had been compromised)

- Greater emphasis on audits (including audits of technology).
- Short privacy notices (while not a substitute for detailed privacy policies) can help bridge the public's lack of understanding
- Using suitable opportunities – such as the November 2005 World Information Summit - to promote privacy/data protection as a universal human right

There was widespread agreement that the question of how Data Protection legislation could cope with future developments in the area of ubiquitous computing and Radio Frequency Identification Devices (RFID's) would need close monitoring.

European Activities

Article 29 Working Party

Opinions and Guidelines issued by the EU Data Protection Commissioners meeting in the Article 29 Working Group provide an invaluable source of guidance both for individual commissioners and for data controllers – especially multinational companies operating in different Member States. Such guidance helps to achieve a more harmonised application of the Data Protection Directives across the EU.

Guidance issued by the Working Group in 2005 covered issues such as use of biometrics in passports, data transfers outside of the EU and the use of location data to provide added-value services. The texts of the guidance documents issued by the Working Group are available on the EU Commission's website at http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2005_en.htm. The guidance on our website (www.dataprotection.ie) has been adjusted as necessary to take account of that provided by the working party.

Data Protection in the Third Pillar

The European Union rests on a number of 'pillars'. The First Pillar includes those areas in which the EU Commission has competence (essentially commerce, the free movement of goods, services and people), the Second Pillar deals with Foreign and Security Policy whilst the Third Pillar is concerned with Justice, Homes Affairs and Civil Protection (JHA). The Data Protection Directive 95/46/EC is a First Pillar instrument and does not automatically apply to Third Pillar areas. Whilst the Irish government decided to apply the provisions of the Directive to the Third Pillar when transposing it into Irish law, this is not necessarily the case across Europe. In 1999, the Treaty of Amsterdam brought certain Third Pillar issues into the First Pillar and also focused attention on intergovernmental cooperation in police, criminal and judicial matters. The Hague Programme of 2004 required the EU Commission to address the issue of 'availability' - that certain data are made available for law enforcement purposes between the competent authorities of member States. As a result, two Framework Decisions are now under discussion in Europe; 'on simplifying the exchange of information and intelligence between law enforcement authorities of the member States of the European Union, in particular as regards serious offences including terrorist acts' and 'on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters'.

My Office has been involved in a working party of European Data Protection Authorities that met on a number of occasions to discuss these framework decisions and develop an opinion on the data protection issues. I welcome the fact that data protection is being considered as an important factor in such legislation and expect that it will be given appropriate consideration in any final instruments dealing with police and judicial cooperation across the EU. I also note the new supervisory role that the framework decision may provide for Data Protection Authorities at national and EU level.

SIS II Developments

The Schengen Information System (SIS) has existed as a mechanism to make information available to parties to the Schengen Convention. This information deals with the movement of people and goods, as well as police cooperation, and supports the purpose of the Schengen Convention to eliminate internal border controls. As SIS was designed to cope with 18 Member States, the enlargement of the EU prompted a redesign of the system. The opportunity has also been taken to include, or allow for later inclusion of, new features into the new SIS II system (due by 2007). Currently, I am an observer at meetings of the Joint Supervisory Authority Schengen, a body which has considered the data protection issues relating to SIS II and offered an opinion to Council.

Ireland is not currently a party to the Schengen Convention, but Council Decision 2002/192/EC of 28 February 2002 allows for Ireland to take part in some of the provisions of the Schengen acquis. Part of any assessment prior to participation will be the ability of a competent national authority (An Garda Síochána) to access SIS II. The development of a national system (nSIS II) is a matter for the Department of Justice, Equality and Law Reform along with An Garda Síochána, and I understand this matter is being progressed. The participation of Ireland in the Schengen acquis will provide additional responsibilities for me and my office, both at home and abroad.

Transborder data flows

The free flow of personal data within the EU is enabled by the presence of adequate EU and national legislation to ensure that privacy rights are respected. EU Directive 95/46/EC seeks, in part, to ensure that when personal data are exported, those data are properly protected. This is achieved by the data exporter meeting at least one of a number of conditions. These conditions are detailed in section II of the Data Protection Acts. An export of personal data that does not satisfy at least one of those

conditions is unlawful. Some of these conditions require the prior approval of this office. Like many other European Data Protection Authorities, this office had experienced few such applications. However, during 2005 that changed and, as a result, I granted this office's first approval for the export of data in late 2005. My office is also actively engaged in other assessments, including approval of Binding Corporate Rules (BCR). BCRs, as well as model contracts, are means by which EU citizens can continue to have their rights protected when their data are exported outside of the EU.

Administration

Running Costs

The costs of running the Office in 2005 were as follows:

	2004 (€)	2005 (€)	increase
Overall running costs	1,323,676	1,391,782	5%
Receipts	530,854	573,421	8%

A fuller account of income and expenditure in 2005 is provided in Appendix 3.

Staffing

The full authorised compliment of staff for the Office is 21. At the end of the year there were 5 vacant posts.

Part 2 - Case Studies

- | | | | |
|-----------|--|-----------|---|
| 26 | 1. Biometric time and attendance system | 34 | 6. Cross marketing of a credit card by a travel agent |
| 28 | 2. Life assurance company and medical reports – access request denied | 35 | 7. Complaint against AIB - excessive information sought regarding Savings Account |
| 30 | 3. Access request - legal advice that it should not be granted because of High Court proceedings – compliance following intervention by Office | 36 | 8. CCTV cameras on the Luas line |
| 31 | 4. Complaint by School Manager about disclosure to parents of his personal data contained in a school inspection report | 37 | 9. Disclosure of patient details to the National Treatment Purchase Fund |
| 33 | 5. Form of Authorisation in relation to applications under statutory housing schemes | 38 | 10. Optic Communications – persistent unsolicited marketing phone calls |
| | | 39 | 11. Prosecution of 4's A Fortune Ltd – unsolicited communications |
| | | 41 | 12. Night club – collection of mobile numbers for marketing purpose |

CASE STUDY **One**

Biometric time and attendance system

A number of staff at a public institution submitted complaints that the biometric time and attendance system installed involved an unreasonable intrusion on their privacy. The Data Protection issue at stake was whether a biometric system for such a purpose, involving a central database, was proportionate.

Guidance on our website (www.dataprotection.ie) invites employers to examine critically the justification for the introduction of a biometric based system and to address issues such as the following:

- Do I have a time management and/or access control system in place?
- Why do I feel I need to replace it?
- What problems are there with the system?
- Are these problems a result of poor administration of the system or an inherent design problem?
- Have I examined a number of types of system that are available?
- Will the non-biometric systems perform the required tasks adequately?
- Do I need a biometric system?
- If so, what kind do I need?
- Do I need a system that identifies employees as opposed to a verification system?
- Do I need a central database?
- If so, what is wrong with a system that does not use a central database?
- What is the biometric system required to achieve for me?
- Is it for time management purposes and/or for access control purposes?
- How accurate shall the data be?
- What procedures are used to ensure accuracy of data?
- Will the data require updating?
- How will the information on it be secured?
- Who shall have access to the data or to logs?
- Why, when and how shall such access be permitted?
- What constitutes an abuse of the system by an employee?
- What procedures shall I put in place to deal with abuse?
- What legal basis do I have for requiring employees to participate?
- Does the system used employ additional identifiers (e.g. PIN number, smart card) along with the biometric?
- If so, would these additional identifiers be sufficient on their own, rather than requiring operation in conjunction with a biometric?
- How shall I inform employees about the system?

Proportionality requires that processing of personal data, in view of its specific purposes, should be appropriate and be the minimum necessary to achieve the stated purposes.

- What information about the system need I provide to employees?
- Would I be happy if I was an employee asked to use such a system?

In its response, the institution pointed to its responsibility for safeguarding the valuable public assets under its control. It stated that the introduction of a biometric system was an outcome of a security review process.

In investigating this matter, my staff sought to establish the nature of the biometric data involved, as biometric data relate to the physiological characteristics of an individual and may facilitate his or her unique identification and linkages with other databases. They also required the institution to provide detailed information in relation to the security safeguards which were in place to protect the privacy of the employees' personal data stored on the system.

It was established that the information collected on the system is held in encrypted code and is derived from a person's finger. This template is then stored for subsequent authentication on the reader and on the Time Management System database. The institution also stated that, as a reader is used, rather than a scanner, no picture of a finger print is formed, so that even if the data could be read, it could not be 'reverse-engineered' to re-generate a fingerprint.

The institution indicated that staff had been consulted about the introduction of the biometric system which was 'to provide the (*institution*) and its personnel with a convenient, accurate and secure

means of managing access to and from the (*institution's*) premises and for accurately recording attendance at work.'

In relation to security of the premises, the institution indicated that the biometric system would also improve physical security systems in place, by further restricting access to unauthorised areas of the building, including areas restricted to staff of the institution.

Proportionality requires that processing of personal data, in view of its specific purposes, should be appropriate and be the minimum necessary to achieve the stated purposes and that these be weighed against the intrusion on the employees' privacy rights. In assessing whether the introduction of the biometrics system was proportionate, we took into account several aspects of the circumstances of this case. In particular, we had regard to the concerns of management in relation to the physical security of the premises, including unauthorised access to restricted areas, and the particular circumstances relating to an institution where security is of paramount importance. We also took into account the particular features of the biometric system installed.

In the circumstances, we concluded that the system was proportionate and did not constitute an unjustified interference with the privacy rights of individuals.

The case highlighted the meaning of proportionality in practice.

CASE STUDY **Two**

Life assurance company and medical reports - access request denied

I received a complaint from a data subject who had not been given copies of medical reports, commissioned from independent specialists by a life assurance company in connection with her on-going income continuance claims – the Company had discontinued her claims on the basis that she was no longer fulfilling the definition of disability, as required under her policy.

In investigating this complaint, I reiterated that the Data Protection Acts give people a statutory right of access to their data, including their medical records, and that this right can only be limited or set aside in very specific and narrow circumstances.

The Company had cited the exemptions in section 5(1)(f) and 5(1)(g) as a basis for denying access to certain reports.

Section 5(1)(f) of the Acts provides that the right of access to personal data does not apply to personal data:

“(f) consisting of an estimate of, or kept for the purpose of estimating, the amount of liability of the data controller concerned on foot of a claim for the payment of a sum of money, whether in respect of damages or compensation, in any case in which the application of the section would be likely to prejudice the interests of the data controller in relation to the claim.”

I considered that medical reports commissioned by a life assurance company are for the purpose of assessing a claim. I found that the exemption in section 5(1)(f) permits a data controller, who puts on file an estimate of the amount of money that may be needed to meet a claim for compensation, to plead an exemption if the release of that estimate would be prejudicial. The contents of the medical reports at issue in this case did not relate to estimating liability per se. Rather, they related to

whether or not there is a disability and opinions about capacity to work. It was therefore my view that this exemption cannot be claimed in respect of medical reports.

The company also proposed to withhold other reports on the basis of legal privilege as provided in section 5(1)(g), as they believed that they would ‘seriously prejudice (their) defence in any action’. Section 5(1)(g) provides that the right of access to personal data does not apply in respect of data :

“(g) in respect of which a claim of privilege could be maintained in a court in relation to communications between a client and his professional legal advisers or between those advisers.”

In assessing whether privilege could be claimed, it is necessary to look at **the purpose** of the referral to the doctor and specifically whether it was in anticipation of legal proceedings or to obtain legal advice. My staff outlined to the Company that it is important when a life assurance company commissions a report that the claimant fully understands the purpose of the examination e.g. the purpose being for the company to assess and to come to a decision on a claim. Whether the reports were commissioned **in anticipation or furtherance of litigation** and thus attract privilege, falls to be determined on a case by case basis.

In assessing whether privilege could be claimed, it is necessary to look at the purpose of the referral to the doctor and specifically whether it was in anticipation of legal proceedings or to obtain legal advice

It was understood that the decision in this case might ultimately be challenged in court and the Company indicated that in their opinion there was a high likelihood of this. The exemption refers to a potential situation where *'a claim of privilege could be maintained in a court in relation to communications between a client and his professional legal advisers or between those advisers'*. In this case, my staff considered that it was conceivable that such a claim could be maintained in a court. Therefore, it was held that certain medical reports specified by the company may be withheld pursuant to section 5(1)(g) pending any court proceedings.

This case shows how the balance between a data subject's right of access to personal data must be balanced with the legitimate interests of a data controller – in this case one who may possibly be facing litigation. In the event of litigation not taking place, the data controller would be required to review its decision.

CASE STUDY **Three**

Access request - legal advice that it should not be granted because of High Court proceedings - compliance following intervention by Office

I received a complaint from an employee of a residential care school, regarding the apparent failure of the school to comply with a request for access to personal data held by the school relating to him.

I pointed out to the data controller that under section 4 of the Data Protection Acts, an individual is entitled to obtain from any data controller, upon request in writing, a copy of all personal data relating to him held by the data controller on computer or in a relevant filing system. This right of access is subject only to some very limited exceptions as specified in the Acts (such as where allowing access would impair the investigation of an offence, or would cause serious harm to the individual's physical or mental health).

My staff asked:

- whether the school held any personal data relating to the data subject at the time of his access request,
- if so, why those details had not yet been provided to him, and if not, why he had not been informed
- what action, if any, they now proposed to take to address this matter.

The Data Controller indicated that the complainant had a personal injuries action pending. He had sought voluntary discovery of various documents relating to his claim. The Data Controller had agreed to comply with the request for voluntary discovery which had the same effect as a High Court order. On the basis of their legal advice, the Data

Controller submitted that the invoking of the jurisdiction of the High Court precluded the data subject from using the Data Protection Acts' subject access provision as 'a parallel process' to obtain documentation and that his request for access to his personnel file was premature given that there were High Court proceedings in being.

My staff pointed out that there is no provision in section 4 or section 5 restricting access to personal data which might impact on forthcoming proceedings, other than data in respect of which a claim of privilege could be maintained. They indicated that they did not accept that, as the data subject had invoked the jurisdiction of the High Court, he was precluded from using data protection legislation as a '*parallel process*' to obtain documentation. The Acts require the data controller to provide the data subject with access to his personal data unless one of the exemptions in section 5 applied.

Having taken legal advice, the Data Controller agreed to comply with the access request.

This case shows that a Data Controller must have a clear statutory basis for refusing an access request.

there is no provision in section 4 or section 5 which restricts access to personal data which might impact on forthcoming proceedings, other than data in respect of which a claim of privilege could be maintained

CASE STUDY **Four****Complaint by School Manager about disclosure to parents of his personal data contained in a school inspection report**

A School Manager complained to me about disclosure to the school Principal of his personal data contained in the report of an unannounced visit by a school inspector under the terms of the Education Act 1998.

Comments about a School Manager or staff member in a school inspection report are personal data relating to that individual within the meaning of the Data Protection Acts.

In this case, the inspection report was released to the school principal, in response to an application by her to the Chief Inspector requesting a review of the inspection under section 13(9) of the Education Act 1998. The Department of Education and Science indicated that their policy in relation to the publication of inspection reports is as follows:

'It is the Department's practice to provide a copy of an inspection report to a person seeking a review as part of the section 13(9) Review Procedure process. It is the view of the Department that the report in question was a record which was required to be disclosed to that person by operation of a rule of law, and in accordance with section 8 of the Data Protection Act, such disclosure is exempt from the terms of that Act and consequently the prior consent of a data subject was not required.'

My Office informed the Department that, insofar as possible, inspection reports which issue should not contain third party data, or at least that party's consent should be sought to permit disclosure of his or her personal data, other than in cases under section 8(e) and 8(f) of the Data Protection Acts. In effect, these provisions allow for disapplying the restrictions on disclosure where required 'by or under an enactment or a rule of law or order of a court', section 8(e), or where 'required for the purposes of or in the course of legal proceedings in which the person making the disclosure is a party or a witness', section 8(f).

My Office advised the Department of their obligations under the Data Protection Acts, in particular of the general requirement that, in any case where an individual's rights might be prejudiced, that that person should be made aware in the event that their personal data are being disclosed to a third party.

I also received complaints from the same School Manager, the Principal and a teacher about the release of the report to parents under the Freedom of Information Acts. Under Freedom of Information legislation, personal information is exempt from disclosure to third parties, subject to a number of exceptions. These exceptions include where the public interest in disclosure outweighs the individual's right to privacy. Section 28(5)(a) of the Freedom of Information Acts provides that a request for third party personal information may be granted when '*on balance, the public interest that the request should be granted outweighs the public interest that the right to privacy of the individual to whom the information relates should be upheld*'. This is an exception and the Information Commissioner has ruled (case No 99001) that '*the protection of personal privacy afforded by the section 28 exemption is intended to be a strong one*'.

My staff considered the issue of the interface between the Freedom of Information Acts and the Data Protection Acts. Section 1(5)(a) of the Data Protection Acts 1988 and 2003 provides that -

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

The key issue in deciding whether a disclosure of personal information under the Freedom of Information Acts is legitimate in so far as the Data Protection Acts is concerned is the question of the public interest in each case

The Data Protection Acts also set aside the general prohibition on disclosure in a number of specified circumstances including where disclosure is required under an enactment or by a rule of law or a court order.

In assessing whether a disclosure of personal information under the Freedom of Information Acts is legitimate in so far as the Data Protection Acts is concerned, the key issue is to determine what is the public interest in the particular case, and to apply the test provided by section 28(5)(a) of the Freedom of Information Acts. In the present case, this Office considered that there was a legitimate public interest, from the perspective of transparency and accountability, in a School Inspector's report being made available to parents and that this public interest outweighs the right to privacy of the individual to whom the information relates. Accordingly, my staff concluded that there had not been a contravention of the Data Protection Acts.

I am aware that the Minister for Education is making School Inspection reports publicly available in the interests of transparency. My Office has advised that care should be taken to ensure that only personal data which is essential to the substance of the Inspection Report should be included.

CASE STUDY **Five**

Form of Authorisation in relation to applications under statutory housing schemes.

I received a complaint from a member of the Dáil, who had concerns about the privacy implications of forms of authorisation which applicants for local authority housing were required to sign.

The forms enabled local authorities to undertake such investigations as they deemed necessary, in order to ascertain the bona fides of applicants housing circumstances, and applicants for local authority housing were required to indicate that they did not object to these enquiries.

My Office looked into this matter, and the position is that there is a statutory basis for making these enquiries, under section 15 of the Housing (Miscellaneous Provisions) Act, 1997. This provides that a local authority, for the purposes of its functions under the Housing Acts, may request and obtain information from the bodies listed therein, including the Gardaí, the Department of Social and Family Affairs, and housing authorities. I therefore had to inform the Deputy that, as the local authority's action was explicitly provided for by law, no contravention of the Data Protection Acts was involved.

This case illustrates the importance of examining the privacy implications of legislative proposals before they are enacted.

the importance of examining the privacy implications of legislative proposals before they are enacted

CASE STUDY **Six****Cross marketing of a credit card by a travel agent**

I received a number of complaints against Stein Travel about the marketing of a Stein Travel/MBNA credit card. It transpired that Stein Travel had provided all the relevant contact data of its customers to MBNA.

When my staff enquired about this, Stein Travel were of the opinion that they were compliant with the Data Protection Acts in conducting their campaign. On their booking form under the heading of Data Protection it is stated that *'The information that we use is for fulfilling our contract as a tour operator/holiday provider. We may from time to time, make your information available to companies within our group.'*

As MBNA was not a company within the group and as marketing a credit card is not the same as marketing a holiday, it was held that consent from customers should have been obtained prior to the marketing of the Stein Travel/MBNA credit card. When this was brought to Stein Travel's attention, they initiated an immediate cessation to the campaign and undertook to review their entire procedures relating to storing and processing data and their marketing practices where promotional partners are involved.

My staff also contacted MBNA who stated that they had assumed that the necessary consents had been given by Stein Travel customers to receiving calls about the credit card. I accepted this and that MBNA had acted in good faith.

In this case, I was satisfied that Stein Travel acted promptly to revise their procedures and I was happy that they were now aware of their responsibilities under the Acts.

The case illustrates the importance of being clear about marketing practices - a credit card, even a co-branded one, is not considered by me to be a product or service similar to the principal business. In these circumstances, the onus is on the travel agent to ensure that consent is given for this type of direct marketing.

a credit card, even a co-branded one, is not considered by me to be a product or service similar to the principal business.

CASE STUDY **Seven**

Complaint against AIB - excessive information sought regarding Savings Account

I received a complaint against AIB Bank that unnecessary personal data relating to employment and salary were asked for by the Bank on opening a Savings Deposit Account.

My Office took this up with the Bank, acknowledging that the Bank has responsibilities under the Criminal Justice/Money Laundering Act to collect a certain amount of data when an individual is opening a bank account e.g. name, address, previous address, date of birth, gender. However, the Bank was advised that personal data relating to the individual's employment and salary would be considered by this Office to be excessive data when opening this type of an account, having regard to section 2(1)(c) of the Data Protection Acts which provide that data **'shall be adequate, relevant and not excessive'** in relation to the purpose for which it is kept.

The Bank stated that its purpose in collecting the information was to *'allow us to shape our relationship with the customer into the future. It also gives us the opportunity to inform customers on the automated/electronic options available to them to meet their daily banking needs, while simultaneously giving them the comfort of knowing that they can contact their relationship manager for any of their future financial needs. By operating a customer consultant fact-find process when opening new accounts, we can better assess the customers financial needs now and in the future'*.

Following further correspondence, the Bank advised this Office that they had circulated training manuals to all branches in November, 2005 highlighting the

difference between mandatory information and information that would be excessive to ask for. In addition, the Bank informed this Office that a new Savings Account opening form was to be launched in February 2006.

I was satisfied that the Bank were aware of their responsibilities under the Acts and appreciated the prompt manner in which they addressed this issue.

The guiding principle always must be that no more information than is necessary for the purpose should be collected from the data subject.

The guiding principle must always be that no more information than is necessary for the purpose should be collected from the data subject.

CASE STUDY **Eight**

CCTV cameras on the Luas line

I received a complaint concerning one of the CCTV cameras on the Luas line which the complainant stated completely overlooked his back garden, giving rise to the feeling that the family were under constant surveillance and were unable to enjoy their private property because of the presence of the camera.

Connex, the Luas operators, acknowledged that the camera could indeed monitor parts of the complainant's back garden. My Office indicated that the rules of data protection require that personal data recorded must be relevant and not excessive for the purposes for which it is obtained. In relation to CCTV cameras, this means that the camera must be positioned so that it cannot capture non-relevant images in its vicinity.

Connex informed this Office that their policy in relation to CCTV was that cameras are to be used to monitor public areas and should not be used to monitor private areas. They agreed that the camera in question could monitor sections of the complainant's back garden. The Commissioner therefore directed that Connex immediately take the necessary steps to rectify the matter so that the camera's range makes it impossible to enable monitoring - albeit inadvertent - of the complainant's private property.

Connex then modified the system so that the camera /monitor was now showing a black screen when moving over the private property in its range. They also said that these settings cannot be changed by the personnel who are using the cameras and monitors in the Central Control Room of Connex.

I was satisfied that this solution resolved the issue and that Connex were now aware of and fulfilling their obligations and responsibilities under the Data Protection Acts.

this means that the camera must be positioned so that it cannot capture non-relevant images in its vicinity.

CASE STUDY **Nine**

Disclosure of patient details to the National Treatment Purchase Fund

I received a complaint from a public hospital patient whose data had been disclosed to the National Treatment Purchase Fund (NTPF).

My staff noted that regulation 4(b) of Statutory Instrument 179 of the 2004 National Treatment Purchase Fund Board Establishment Order 2004 states –

“Without prejudice to section 52 of the Health Act, 1970 the functions of the board are as follows :

(b) to collect, collate and validate information in relation to persons waiting for hospital treatment and to put in place information systems and procedures for that purpose”.

As the hospitals had collected the patient data for the purpose of patient treatment, it was considered that disclosure to the Fund is compatible with the purpose for which the patients had given their data to the hospital in the first place. Furthermore, the transmission of the data was for a statutory purpose relating to treatment. It was therefore considered that disclosure of data to the NTPF Waiting List Register was compatible with the purpose for which hospitals hold the data and therefore satisfied section 2(1) of the Data Protection Acts.

It was also considered that section 2A(1)(c)(iv) provides a basis for disclosing the data. This provides for processing of personal data (defined to include ‘disclosure’) necessary *“for the performance of any other function of a public nature performed in the public interest by a person”.*

As the data includes sensitive personal data as to health, one of the conditions specified in section 2B must also be satisfied. In this regard section 2B (1)(b)(vi)(11) provides that sensitive data shall not be processed (defined to include ‘disclosure’) unless, inter alia,

“the processing is necessary -

(11) for the performance of a function conferred on a person by or under an enactment”.

I was of the view that this allows the National Treatment Purchase Fund to collect information in respect of persons on waiting lists in order to manage and facilitate their treatment and that this was compliant with the Acts.

The National Treatment Purchase Fund had consulted my Office about this process and our advice was that patients should be informed that the disclosure had been made and given the opportunity to have their data deleted by the Fund. This advice was implemented. It is important to also emphasise that the Waiting List Register does not involve the publication of personal data. Only the National Treatment Purchase Fund and the relevant hospital (in respect of its own patients) has access to specific personal data.

this allows the National Treatment Purchase Fund to collect information in respect of persons on waiting lists in order to manage and facilitate their treatment and this was compliant with the Acts.

CASE STUDY **Ten****Optic Communications - persistent unsolicited marketing phone calls**

Given that compliance is my primary objective, I did not consider that it warranted initiating Court action when the problem appeared to be resolved.

The marketing activity of a telecommunications service provider caused a number of complaints to be made to my office in the middle of the year. It was claimed that Blueridge Telecom Systems, trading as Optic Communications (Optic), was making persistent marketing phone calls despite being told not to call again.

In all cases the complainants were businesses who had instructed Optic by phone, fax or mail that they did not want to be called again but who were still in receipt of such clearly unsolicited phone calls. This is contrary to Regulation 13(4) (a) of Statutory Instrument 535 of 2003, which states

*" A person shall not use, or cause to be used, any publicly available electronic communications service to make an unsolicited telephone call for the purpose of direct marketing to the line of a subscriber, where -
the subscriber has notified the person that the subscriber does not consent to the receipt of such a call on his, her or its line".*

A failure to comply with Regulation 13(4) (a) is an offence for which the offender can face prosecution by this Office. It is also worth noting that this Regulation applies to both natural persons and to business users of phones. This is the first time that data protection rights have been provided to non-natural persons.

Upon investigating the matter it became clear that, in certain cases, Optic Communications had contacted businesses without consent. However, a number of issues caused problems for my investigation. In some cases, although head offices had clearly instructed Optic Communications not to contact them, Optic later phoned branch offices which referred them to head office. Optic took these referrals as overriding earlier instructions from the head office. This is a farcical and simplistic approach, but could result in sufficient doubt being created that a Court would be reluctant to convict the defendant.

A more serious problem was the nature of Optic's presence in the State. Although Optic is authorised

to provide a telecommunications service in this State, it is not required to have a physical presence here. Optic uses another Telecommunications Service Provider in order to provide a service to its customers and uses a Dublin postal address to forward mail to its head office in the USA. Optic argued that it was not and is not subject to Irish data protection law in that it is not established in Ireland and in that the marketing calls in question were made from either the USA or Egypt.

I informed the Commission for Communication Regulation that the system for authorising telecommunications service providers was resulting in difficulties for my office where the service provider had an unclear presence in this State. Whilst accepting that this new system may have been desirable in order to deregulate the telecommunications sector, it appears to have had one undesirable consequence.

Notwithstanding this, I was satisfied that I could still take enforcement action against Optic through its agent(s) in this State, though this would still be difficult. However, as a result of the actions of my office and of ComReg, Optic ceased all telephone marketing operations on 1 September 2005. Given that compliance is my primary objective, I did not consider that it warranted initiating Court action when the problem appeared to be resolved.

It may be worth noting that my office was also the target of such calls from Optic and that these calls were persistent, aggressive and at times abusive in content. I find it difficult to see how a company could expect to sell a service using such techniques and hope that other companies engaged in telephone marketing pay more respect to their potential customers.

CASE STUDY **Eleven**

Prosecution of 4's A Fortune Ltd - unsolicited marketing communications

A number of complaints were made to my office in March 2004 about a marketing campaign that promoted a game of fortune by contacting mobile phones. In all cases, the mobile phone rang briefly and did not allow the complainants adequate time to answer before the call terminated. A 'missed call' was recorded and the phone listed a Dublin based fixed line number. When a person phoned that number, a pre-recorded message was played in which callers were invited to phone a premium rate number in order to avail of an offer to claim €50 credit for use in the 4's A Fortune game.

The provisions of Statutory Instrument 535 of 2003 [European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2003] took effect in November 2003. Regulation 13 refers to unsolicited communications, making it an offence in certain circumstances to make marketing calls or send marketing messages. The campaign under investigation effectively resulted in a 'call me' message being left on subscribers' phones, the sole purpose of the message being to encourage subscribers to phone another number and thereby receive a direct marketing message. This was contrary to Regulation 13(1)(b) which states

"A person shall not use or cause to be used any publicly available electronic communications service to send an unsolicited communication for the purpose of direct marketing by means of electronic mail, to a subscriber, who is a natural person, unless the person has been notified by that subscriber that for the time being he or she consents to the receipt of such a communication".

As failure to comply with Regulation 13(1)(b) is an offence, once I had decided that an offence appeared to have been committed, it was necessary to gather all relevant material and then make an assessment of whether or not a prosecution was appropriate. Despite indications of cooperation from the data controller, it was still necessary to obtain evidence in case the matter was brought to Court. I exercised my powers to issue Information Notices to a number of telecommunication service providers to

establish the ownership of the phone numbers involved in the campaign, as well as to establish whether those numbers had contacted the complainants' phone numbers during the period under investigation.

The phone numbers used in the promotion were registered to Realm Communications Limited, and these lines were used on behalf of 4's A Fortune Limited for the purpose of this promotion. Both companies shared the same premises. It was also established that 165,000 calls were made during the promotion and that the complainants' numbers had been phoned by Realm Communications / 4's A Fortune. With this evidence, it appeared that there was a substantial case to be answered. Two of my authorised officers visited the offices of Realm Communications / 4's A Fortune in order to question the director Mr Tom Higgins. As he was not present, the officers went to his home address. Although Mr Higgins was preparing for a press conference on an unrelated matter, he still found time to discuss the matter. As a result of that meeting, Mr Higgins attended my office and volunteered a statement under caution. He also indicated a willingness to enter a guilty plea if the matter came to Court.

Following assessment of all the material, it was decided that there was sufficient evidence to demonstrate that an offence had been committed in respect of five of the complainants. In the case of the other four complainants, there were doubts over the existence of consent to make those calls and doubts over whether calls had been made. It is

I am satisfied that this case has sent a positive signal to marketers that I will not be reluctant to prosecute those who fail to respect the privacy rights of others.

important to note that although I had evidence that the campaign involved the contacting of 165,000 subscribers, I can only prosecute in those cases where there is no consent from the recipient to receiving such calls. Therefore, I am restricted to prosecution in relation to specific complaints from individuals.

In March 2005 summonses were issued in respect of five offences and 4's A Fortune Limited entered guilty pleas in July 2005. At the final hearing at Court 54 on 1 September 2005, 4's A Fortune was convicted of committing five offences of failing to comply with Regulation 13(1)(b) and fined €300 out of a maximum of €3,000 on each count, plus costs of €1,000.

This was the first prosecution brought under these Regulations. The technical nature of the evidence required was a factor in the time taken to finalise the investigation, but I believe that the experience gained from this case will result in speedier investigations in future. I am pleased to note that the level of complaints relating to marketing to mobile phone numbers has declined significantly since this case was publicised and am satisfied that this case has sent a positive signal to marketers that I will not be reluctant to prosecute those who fail to respect the privacy rights of others.

CASE STUDY Twelve

Night club - collection of mobile numbers for marketing purpose

This is a classic example of a business being attracted by new technology without making itself aware of its legal responsibilities.

There is a noticeable increase in the use of text marketing services as a promotional tool in the retail and leisure sectors. During 2005 a number of such promotions were the subject of complaints to my office and I will focus on one particular example in order to highlight the potential problems.

In the second half of the year an individual contacted my office to complain about the receipt of text messages on her mobile phone. These messages promoted a night club in Dublin, but the caller did not live in the locality and had never visited the establishment. The sending of text messages contrary to Regulation 13(1) (b) of Statutory Instrument 535 of 2003 is an offence. That states

“A person shall not use or cause to be used any publicly available electronic communications service to send an unsolicited communication for the purpose of direct marketing by means of electronic mail, to a subscriber, who is a natural person, unless the person has been notified by that subscriber that for the time being he or she consents to the receipt of such a communication”.

As neither the complainant nor any of her family had any association with the night club, I asked the data controller to explain what justification he had to send such messages. In his reply, the data controller stated that the complainant's number had been obtained during an in-club promotion. This conflicted with the complainant's account and so I decided to send authorised officers to inspect the night club records.

The inspection found that mobile phone numbers were collected when patrons of the club filled out a form that was passed around on given nights. This is not a very privacy friendly way of collecting such details. Aside from the fact that patrons can read details belonging to other patrons, because of the nature of the venue certain patrons might not be in a proper condition to give consent to the use of

their personal data. It is also easy for a patron to accidentally or deliberately write down the wrong number, or for staff to transcribe the number inaccurately onto a marketing database.


The company had already taken some remedial action. It had removed the complainant's details from its marketing list and had provided a new number for customers to text if they wanted to opt out of future marketing. I recommended that the company look at replacing the manual form of data collection with an electronic one, such as asking customers to phone/text a number. In this way a number would be automatically and correctly recorded. This would prevent inaccuracies relating to numbers. I further suggested that the data collection should be done at an early stage in the evening, when patrons would be more likely to be aware of the implications of entering a promotion.

This is a classic example of a business being attracted by new technology without making itself aware of its legal responsibilities. Whilst the legislation doesn't differentiate between the casual marketer and the professional, I was not inclined to prosecute this company. The company admitted responsibility and took remedial action and I am satisfied that the company will behave in a more responsible manner in future.

This type of behaviour is becoming more common and if the sector continues to ignore its responsibilities, in future I may have no choice but to engage in enforcement action.



Part 3 - Guidance

- 44 Guidance Notes
 - 44 Community CCTV Cameras
 - 44 IFSRA Consumer Code
 - 45 Motor Dealers
 - 45 Electoral Acts – use of Complete Register of Electors
 - 46 Putting Planning Submissions on the Web
- 

Guidance

Guidance Notes

One of the core functions of the Office is to provide guidance on how data protection principles should be applied in practice in particular settings.

Extensive guidance is provided on our website (www.dataprotection.ie). The guidance notes on the site were updated in the course of the year, and some new guidance was added – notably in relation to direct marketing and the telecommunications sector.

We are also regularly consulted by data controllers faced with particular data protection issues. We welcome such contact and are happy to sit down with individual controllers and work through the issues that face them. We much prefer to resolve issues at an early stage rather than be faced with complaints about the conduct of data controllers at a later stage.

The following paragraphs give some examples of the guidance we provided in the course of 2005 to particular data controllers.

Community CCTV cameras

The Office was consulted by the Department of Justice, Equality and Law Reform on the Data Protection issues surrounding the proposed Community CCTV cameras scheme. The definition of personal data in the Data Protection Acts 1988 and 2003 is -

“data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller”.

The presumed objective of recording images is that they are capable of being personalised. Modern cameras can be operated to zoom in closely on particular incidents, areas and individuals and operators will be capable of identifying individuals from the images, particularly so in areas where

community CCTV schemes are operating. In these circumstances, it was considered that images that potentially identify individuals are caught by the above definition.

The Department enquired as to whether section 8 of the Data Protection - which provides that any restrictions on the processing of personal data do not apply if the processing is required for the purpose of preventing, detecting or investigating offences - provided an exemption for Community CCTV cameras. However, it was pointed out that this exemption is subject to a case by case prejudice test which must be satisfied - it applies only ‘in any case in which the application of those restrictions would be likely to prejudice any of the matters aforesaid’.

This Office indicated that it supported the proposal that the operation of Community CCTV cameras be given a statutory basis. This was subsequently done in section 38 of the Garda Síochána Act, 2005. We also indicated that we would welcome the adoption of a Code of Practice relating to Community CCTV cameras. Such a Code was published by the Department in June 2005 and is available on its website (www.justice.ie).

IFSRA Consumer Code

The Office was consulted in regard to the Irish Financial Services Regulatory Authority's draft Consumer Protection Code Consultation Paper CP10 (February 2005).

We were pleased to note that the draft Code covered the data protection principles contained in the Acts in a satisfactory manner, even though it does not specifically seek to address data protection requirements. We were particularly happy to note the intention to ban ‘cold calling’ in relation to all financial services.

One of the key obligations of the Acts in section 2D is that data subjects (individuals) should be informed, for

the sake of transparency, about the nature and purposes of data processing in order that personal data can be considered to be 'processed fairly'. We asked that consideration be given to a number of points that would enhance transparency, particularly that each customer be given a description of the purposes for which personal data are intended to be processed and the persons or categories of persons to whom the data may be disclosed.

The final text of the Code is due to be published in July 2006.

Motor Dealers

We were consulted by the Society of the Irish Motor Industry regarding the question of direct marketing of customers by vehicle manufacturers.

It was made clear that any marketing must be done with the consent of the customer.

In regard to retention of data about prospective customers, my office emphasised that a customer has the right to be told that the Dealer is retaining the data for marketing purposes, and has the right to opt out. If the Dealer is contractually required to make that data available to the distributor, s/he has a right to be told this and to opt out also. A contractual obligation to a third party cannot over-ride the need for individual consent – the minimum acceptable level of consent being an opt-out. A data subject has a right under section 2D of the Data Protection Acts 1988 and 2003 to be given details of -

- (a) the identity of the data controller,
- (b) the purpose or purposes for which the data are intended to be processed, and
- (c) any other information necessary for 'fairness', such as information as to disclosees, whether questions are compulsory and information about the individual's right of access to data.

Equally, when a customer buys a car, the marketing opt-outs must be available to the customer. There is no problem with personal data necessary for warranty or recall purposes being passed to the distributor but these data can only be processed for these purposes – marketing purposes will require consent, as explained above.

Electoral Acts – use of Complete Register of Electors

The Department of Social and Family Affairs sought clarification about that Department's entitlement to obtain access to the complete Register of Electors.

The Electoral (Amendment) Act 2001 provides for the preparation of an edited version of the Register of Electors which omits -

'the names and addresses of registered electors or electors on whose behalf requests have been made that their details should not be used for a purpose other than an electoral or other statutory purpose'.

It was indicated that it had always been the view of this Office that, when other uses are planned in relation to personal data beyond those for which the data were collected, then this should be provided for by specific legislation. The primary purpose of the electoral register is to facilitate voting and it is our understanding that 'other statutory purpose' would refer to a specified purpose in a specific statute.

Section 222 of the Social Welfare (Consolidation) Act, 1993 provides that -

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

or a specified body may be transferred by that Minister of the Government or a specified body to the Minister”.

It was the view of the Office that this is a general provision for the exchange of data between the Department of Social and Family Affairs and other Departments, and vice versa, for the specific purposes of the control of Social Welfare schemes in specific cases where there would be a substantial risk that public funds could be abused, **rather than a mere chance**. It was not considered that this section provided a basis for the routine disclosure of the Electoral Register to the Department of Social and Family Affairs.

Similarly, we advised a number of commercial entities that using the complete Register to update existing marketing databases would not, in our view, be legitimate.

Putting Planning Submissions on the Web

The key message that this Office tries to promote is that personal privacy is important and that, within the limits prescribed by law, public authorities should do their best to respect this.

The Office fully accept that the law prescribes - in the interests of transparency and accountability - that submissions in planning matters must be publicly available and that anybody is entitled to ask to inspect the planning file containing such submissions and to be provided with a copy. As long as people are aware of the fact that their submissions will be made public, we have no problem with this practice.

What the Office does have an issue with is the placing of such submissions in their entirety on a web-site. This point is made more clearly in Case Study 6 (on page 28) of our 2004 Report: ‘This reflects the important principle that even where there is legislation providing that information must be made available to the public, this may not always mean that

it is appropriate to place such information on a website full details will still be available for public inspection at the Council Offices as is required by legislation’.

Where details of submissions are being placed on a website - thus being made available to a potentially huge audience - our advice is that the minimum of personal information should be disclosed. In our opinion, it should be sufficient in such cases to give the name and address of the person concerned. It should not be necessary for the general public (as opposed to Council officials) to have the phone numbers of the people concerned - the scope for abuse (e.g. in the form of harassing phone calls) is obvious in such cases.

Where submissions are being scanned in order to be placed on a website, our advice is that any phone/e-mail contact details contained in them should first be ‘blacked out’. While this involves extra work for already hard-pressed Council officials, we believe that the effort involved is worthwhile in order to protect the privacy of the people concerned.



Appendices



- 48 Appendix 1 - Presentations
- 49 Appendix 2 - Registration Statistics
- 50 Appendix 3 - Account of Income and Expenditure

Appendix 1

Presentations

During 2005, 37 presentations were made to some 2,000 people in the following organisations:

Citizens' Advice

Citizen's Information Centre, Tallaght
Comhairle, Dublin – Information Providers Programme
Comhairle, Kilkenny – Information Providers Programme

Commercial

International Association for Information and Data Quality
Irish Centre for Business Excellence
The Insurance Institute of Ireland

Educational Agencies

National University of Ireland – Health Research
Visiting Teachers for Travellers Service

Financial Services

Bank of Scotland (Ireland) Limited
Central Bank of Ireland
Irish Financial Services Regulatory Authority
File Stores & SISI

Health Sector

Health Service Executive – Schemes Administration Project
Health Service Executive – North East Child Care
Irish Cancer Data Association
Trinity College Health Informatics Course

International

European Workplace Drug Testing Society Symposium
International Association of Privacy Professionals

Legal Sector

APD Training – Heslin Ryan & Partners Solicitors
Irish Centre for European Law
Law Society – Employment Law Committee

Mixed Seminars

Enable Technologies Ltd
PricewaterhouseCoopers
The Homeless Agency (2)

State Sector

CMOD – Civil Service Personnel Officers Network
Department of Arts, Sport and Tourism
Institute of Public Administration – HR Management Course
Office of the Director of Consumer Affairs
Ombudsman and Information Commissioners Office
Garda Síochána Training College
Local Government Management Services Board

Telecommunications Sector

Eircom
International Audiotex Regulators Network

Voluntary and Charitable Organisations

Carmichael Centre for Voluntary Groups
Cross Care
Institute of European Affairs

Appendix 2

Registration Statistics 2003/2004/2005

(a)	<i>Public authorities and other bodies and persons referred to in the Third Schedule</i>	2003	2004	2005
	Civil service Departments/Offices	118	127	147
	Local Authorities & VECs	138	144	160
	Health Boards/Public Hospitals	59	60	60
	Commercial State Sponsored Bodies	45	44	45
	Non-Commercial & Regulatory	171	174	178
	Third level	54	50	56
	Sub-total	585	599	646
(b)	<i>Financial institutions, insurance & assurance organisations, persons whose business consists wholly or mainly in direct marketing, providing credit references or collecting debts.</i>			
	Associated Banks	46	46	45
	Non-associated banks	62	66	72
	Building societies	6	7	7
	Insurance & related services	230	303	342
	Credit Union & Friendly Societies	449	445	440
	Credit Reference/Debt Collection	28	35	41
	Direct Marketing	61	65	69
	Sub-total	882	967	1016
(c)	<i>Any other data controller who keeps sensitive personal data</i>			
	Primary & secondary schools	340	572	622
	Miscellaneous commercial	77	130	176
	Private hospitals/health	125	147	149
	Doctors, dentists, health professionals	576	752	850
	Pharmacists	828	850	867
	Political parties & public representatives	108	156	162
	Religious, voluntary & cultural organisations	118	152	186
	Legal Profession	445	615	629
	Sub-total	2,617	3374	3641
(d)	<i>Data processors</i>	524	549	603
(e)	<i>Those required under S.I. 2/2001</i>			
	Telecommunications/Internet Access providers	10	20	27
	TOTAL	4,618	5509	5933

Appendix 3

Abstract of Account of Income and Expenditure for the year 31 December 2005, for the Office of the Data Protection Commissioner

	2004 (€)	2005 (€)
Receipts		
Moneys provided by the Oireachtas	1,323,676	1,392,782
Registration Fees	530,854	573,421
	1,854,530	1,966,203
Payments		
Staff Costs	940,790	937,691
Establishment Costs	269,754	250,224
Education and Awareness	64,814	144,505
Legal and Professional Fees	21,683	46,983
Incidental and Miscellaneous	26,635	13,379
	1,323,676	1,391,782
Payments of Fees to the Vote for the Office of the Minister of Justice, Equality and Law Reform	530,854	573,421
	1,854,530	1,966,203

The financial statements of the Office are subject to audit by the Comptroller and Auditor General and after audit are presented to the Minister for Justice, Equality and Law Reform for presentation to the Oireachtas.