



**Data Protection
Commissioner**

An Coimisinéir Cosanta Sonraí

Annual Report



Tuarascáil Bhliantúil

04



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.

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.*

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.*



Data Protection Commissioner

An Coimisinéir Cosanta Sonraí

Sixteenth Annual Report

of the

Data Protection Commissioner

2004

Presented to each House of the Oireachtas pursuant to section 14 of the
Data Protection Acts, 1988 & 2003

PRN. A5/0451

Contents

03	Foreword
07	Part 1 – Activities
17	Part 2 – Case Studies
33	Part 3 – Guidance Notes
38	Appendices

Foreword

In presenting this sixteenth annual report - my fifth - outlining the activities of the Office of the Data Protection Commissioner for 2004, I feel it is an opportune moment to outline to the Oireachtas my general reflections on where data protection stands in the early part of the 21st century.

Data Protection legislation aims to protect an individual's human right to privacy in the area of personal data processing and is why the Office was established. Personal data protection applies to all our interactions with public and private sector organisation and thus applies to applications, purchases and transactions in state services, business and economic matters, in the social and medical areas, in the workplace and in the globalised technological arena.

While personal data protection is not an absolute right, as it must be balanced with other rights and obligations, it fulfils an important safeguard for human society by ensuring that business and government operate in a fair and transparent manner when processing individuals' personal data.

EU DRAFT CONSTITUTION

Data Protection in the EU has an enhanced basis after the promulgation of the Charter of Fundamental Rights of the European Union by the December 2000 European Council of Nice. Article 8 of the Charter enshrines data protection as a fundamental right of the Union and the existence of fully independent data protection authorities to monitor compliance is an integral part of that right. Article 51 of the Draft Treaty which established a Constitution for Europe, agreed in June 2004, further enhances the basis of data protection by recognising that everyone has the right to the protection of personal data concerning him or her. It also provides that compliance with data protection rules shall be subject to the control of a fully independent authority. Though these are positive developments they must be matched with adequate resources for all the authorities and respect for data protection principles by everyone.

Joe Meade
Data Protection Commissioner



PRIVACY ENVIRONMENT

Protection of personal privacy is always challenging but particularly so if all parties do not operate in an open and transparent manner. To begin with, there needs to be a recognition of the value of data protection as a human right. At the same time, there are few absolutes in life and while data protection and privacy cannot be deemed to be an absolute right, nevertheless technological advances and security requirements must be constantly balanced with a person's data protection rights as established by data protection legislation. I feel that the steps being taken in Ireland to address this 'paradox' are informed and evolving and I expect that there will continue to be dynamic interaction between the various actors involved.

In general people only become concerned about Data Protection rights when they themselves are affected. Government and industry alike should therefore subject any policy proposal or management initiatives to a detailed cost benefit analysis of the effects its proposals may have in the privacy field before they become operational. Such a privacy impact assessment would go a long way to addressing fears about the erosion of privacy rights as it is much easier to build in privacy enhancing solutions at the design stage of a project. The question should always be asked as to whether the envisaged purposes can be achieved by the use of anonymised or pseudonymised data (i.e. data which is reversibly anonymised).

In addition the interaction between data protection and freedom of information is discussed in Appendix 1, while the area of political marketing is considered in Appendix 2.

NATIONAL SECURITY ISSUES

Privacy and security are not diametrically opposed, as appropriate and proportionate national security measures are enhanced by realistic and practical data protection policies. My Office has increasingly had to comment on proposals being brought forward. They include proposals for a framework involving a public sector card, biometrics on passports, dealing with the USA requests for passenger data and financial reporting requirements, as well as consideration of the additional European national security proposals as detailed in the November 2004 Hague Programme. I welcome my comments being sought. I also commend the Law Reform Commission for seeking and taking account of my observations regarding the question of a national DNA databank, as published in their Consultation Paper (LRC CP29-2004).

While consideration of these issues has been resource intensive, it was essential to address them thoroughly as major implications for current and future generations flow from them. I – in common with my colleagues worldwide – am somewhat disappointed that often there is not a fuller appreciation of data protection principles at the initial stage when proposals are being drafted. I recognise however that Governments in particular have difficult choices to make, but increased dialogue with my fellow EU Data Protection Commissioners would be beneficial overall. That is why I suggest above that every proposal – whether at government or industry level – should be subject to a privacy impact assessment test.

Due to the lack of progress at national and EU level on the unsatisfactory legislative basis for the retention of communications traffic data – this was the subject of comment by me in my previous reports – I had no option but to issue enforcement notices in early January 2005 to three telecommunications companies requiring them with effect from 1 May 2005 to hold such data for national security purposes for a maximum period of twelve months. Two of the companies appealed the notices to the Circuit Court while the other did not. I noted that the legislative ‘lacuna’ was being regularised in

that amendments to the Criminal Justice (Terrorist Offences) Bill 2002 were introduced on 3 February 2005 – and subsequently passed – in Seanad Éireann by the Minister for Justice, Equality and Law Reform. As I did not want unnecessary legal costs to be incurred by me or indeed the companies, I cancelled the Enforcement Notices on 7 February in the expectation that this Bill would be enacted before 1 May 2005. Though a three year retention period has been provided in the legislation, I remain of the view that this is an excessive period.

DATA PROTECTION AND THE MEDIA

In line with the EU Directive, Irish Data Protection legislation provides exemptions from its provisions where the processing of personal data is carried out solely for journalistic purposes or for the purpose of artistic or literary expression. However this exemption only applies when the public interest in freedom of expression is considered to outweigh the right to privacy to the extent that publication would be considered to be in the public interest.

Data Protection law therefore recognises the important role of the media, but media must act responsibly. In considering whether publication of the material concerned would be in the public interest, the legislation provides that regard may be had to any code of practice which is either approved by me or indeed brought forward by me – these codes can also be given legal effect. I note the Government is considering the whole area of media coverage, defamation and a possible press council for complaints and I will await developments in this area. In this context I will consider over the next 18 months whether a specific data protection code of practice – to have legal effect – is needed. Such a code would only come about after consultation not alone with media interests but with the general public so as to ensure that it is both balanced and proportionate.

MEDICAL RESEARCH

We all agree that research is necessary in the medical area for the benefit of society. However in the medical research field, personal data is very often processed and the question of consent can on occasions pose problems for researchers and data controllers and data subjects alike. Transparency is vital in this area. The Data Protection Acts allow for medical research to operate in a pragmatic manner but medical researchers have to appreciate that where personal data is being used attention to patients needs is paramount. In this respect, my comments above about anonymisation and pseudonymisation are particularly relevant. I am pleased to record that after constructive discussions with the relevant researchers in the case of a number of important projects - significant changes were made to the original proposals - the following were able to proceed without the research programmes being hindered or reduced:

- *National Parasuicide Register*
- *Coombe Hospital Biobank*
- *Trinity College DNA Project.*

CORPORATE AIM

A regulator's or Commissioner's role is a demanding one which requires fine judgements because while I am endowed with significant powers, it is how I exercise them that determines my overall effectiveness. Persuasion, mediation, dialogue and discourse can be most effective. Recourse to full litigation in many cases may not be effective but my full legal powers can and are exercised when appropriate. I readily acknowledge the efforts being made by many sectors to adhere to data protection principles and my Office aims to deal with matters in a pragmatic and practical manner.

In any organization, systems failures can arise due to a combination of factors including human weakness. However the methods whereby an organisation addresses these weaknesses and brings them to my attention

is a key factor which I take into account when considering whether to use the extensive legal provisions the Oireachtas has granted to me as Data Protection Commissioner.

As well as being the 'Enforcer' of Data Protection, a major part of my role is the promotion of individual awareness of personal data protection rights. Data moves about in ever more complex ways and instantaneously. While organisations generally want to adhere to the Law, in the final analysis, individual vigilance against possible abuses of personal data protection rights is vital so that matters are brought to attention, investigated and best practice ensured. My Office's commitment, therefore, is to address all data protection complaints expeditiously.

REVIEW OF 2004 ACTIVITY

People and organisations continued to be seriously concerned about data protection matters during 2004. The year's activities as outlined later in this Report indicate that more and more people are complaining and contacting the Office. The Office workload increased significantly with additional demands also being made on the Office to provide guidance and talks to organisations that aim to be compliant. We seek to answer and investigate every complaint or inquiry and to give advice and presentations in an efficient manner - Appendix 3 outlines the breadth of our public presentations. Nevertheless choices were made as to what were the priority cases as we cannot deal with every matter as speedily as people would like. An increased numbers of privacy audits and inspections were also carried out, so as to proactively monitor compliance.

Successful prosecutions were taken by my Office - the first ever by the Office since its establishment in 1988. A public awareness campaign was launched to highlight peoples' rights; a training video is being prepared to assist data controllers while a schools competition aimed at transition year second level students was highly successful.

A review by my Office of over 240 state sector websites - Appendix 7- indicated to an alarming degree that the majority of them had either no or inadequate privacy statements. I was very disappointed and concerned at these findings but I am heartened that matters are being addressed. Egovernment and ecommerce will only succeed if people are fully aware as to how their data is being used. I intend to carry out a similar review of private sector web sites in 2005.

My Office is also cooperating at international level in trying to combat 'spam'- Appendix 6 - while prosecutions were initiated in December 2004 for mobile phone text marketing messages. I was somewhat disappointed that ComReg and the communications industry did not have the national opt out register for telephone direct marketing calls operational during 2004.

Registration activity increased overall and the public register is now updated monthly on the Office's website. We are also considering the introduction of online registration if it proves to be cost beneficial but this must await the decision of the Minister regarding future registration obligations.

Guidance notes on specific issues were regularly put on the website during the year and work on the redesign of the website commenced, as we aim for it to be more user-friendly and beneficial.

Finally, due to the decentralisation proposals, opportunity was taken to review office methods and practices, and a new strategy statement and business plan for the period 2004 - 7 was published in June 2004. A relocation plan to provide for a successful decentralisation to Portarlinton was drawn up and is being constantly refined and reviewed.

APPRECIATION

I thank the many people who contacted my Office and brought serious matters to attention. I am appreciative of the majority of data controllers who generally complied fully with the law and who recognized that by


working in a spirit of cooperation with my Office the burdens placed on organisations were minimised.

I again express my gratitude to the Minister for Justice, Equality and Law Reform and his officials for support and the continuing good relations between our Offices even though we may differ occasionally but always in a healthy professional manner.

My Office could not function effectively without the dedicated office personnel who by hard work and professionalism provide an independent and fair public service in as efficient and competent manner as is feasible. I am grateful for their dedication and sound advice given during the year.

ROLE OF THE OIREACHTAS

Though there are many challenges to be faced I am confident that the Office can continue to meet them in an efficient manner. In this respect, I feel the Oireachtas can also play an important and supportive role and I look forward to continuing dialogue with its various committees.



Joe Meade

Data Protection Commissioner

15 March 2005

Part 1

Activities

in 2004

08	Introduction
08	Business Planning Review
08	Customer Service and Promoting Awareness
09	Information for Data Subjects
10	National Directory Database
10	Website, Presentations and Enquiries
10	Complaints and Investigations
12	Public Register
13	Codes of Practice
13	Prosecutions
13	Privacy Audits
14	Advice
14	International Activity
15	Administration

INTRODUCTION

This was the first full year of operation of the Data Protection (Amendment) Act 2003 which took effect from 1 July 2003. The Act, which transposed Directive 95/46/EC into Irish Law, has proved to be a significant piece of legislation, providing a level of privacy protection for personal data which equates with that obtaining throughout the European Union. In a nutshell, the Act clarifies and makes more specific the obligations of data controllers on the one hand and strengthens the rights of data subjects on the other in regard to processing of personal data. Along with the Data Protection Act 1988, the Acts provide a framework for the protection of personal data, overseen by the Commissioner. This framework means that organisations in both the public and private sectors who process peoples' data must do so by following the basic rules which are reproduced in summary form on the inside front cover of this Report. Furthermore, individual data subjects can have their rights vindicated by complaining to this Office, which acting independently, will investigate such complaints. The Commissioner may also act on his own initiative by carrying out audits and inspections to ensure that the requirements of the law in regard to personal data protection are adhered to.

2004 was an extremely busy one for the Office as the following paragraphs indicate.

BUSINESS PLANNING REVIEW

The statistics for 2004 which follow, point to the increased level of demands on the Office in the wake of the new legislation. Given this and our key objective of providing a high standard of customer service to the public, as both data controllers and subjects, the Office carried out a Strategic Review which was completed in the middle of the year. This Review involved consultation with our staff and resulted in the Commissioner adopting a Strategic Plan for 2004 to 2007 and a Business Plan which is to run from July 2004 to end 2005. Both plans were published on our website.

CUSTOMER SERVICE AND PROMOTING PUBLIC AWARENESS

A significant part of the daily work of the Office is focussed on customer service. This involves all staff giving advice to the public and dealing with general enquiries in a prompt and efficient manner. The Business Plan includes specific targets in regard to response times and quality of service and these have now been formalised in our Customer Service Charter, a copy of which is reproduced on our website.

To be effective, public awareness promotion cannot only be reactive. During the year, my Office continued its Public Awareness strategy which entails:

- *Collaboration with and speaking engagements at local Citizen Information Centres.*
- *Interviews on national and local radio and on television.*
- *Participation in trade shows and other events which facilitates face to face contact with the public.*
- *Proactive and reactive engagement with local and national media on Data Protection and related matters.*
- *Targeted advertising on a sectoral and local basis.*

Early in the year, it was decided to focus our promotion efforts on advertising on public transport, and a campaign on buses, the DART and at train stations ran for 6 weeks from mid September. This campaign, judging by the response in terms of telephone enquiries to the office, was highly effective. Samples of campaign:

My middle name is James and the balance in my current account is €438.27


Not everyone needs to know your business. The Data Protection Commissioner is here to ensure that your personal details are kept personal.

 Data Protection Commissioner
An Independent Office of Public Inquiry

For more information go to www.dataprotection.ie or call us on 01876 0544

I got 3 B's in my Leaving Cert and my passport is out of date

Not everyone needs to know your business. The Data Protection Commissioner is here to ensure that your personal details are kept personal.

 Data Protection Commissioner
An Independent Office of Public Inquiry

For more information go to www.dataprotection.ie or call us on 01876 0544

Empowering people to be proactive about their privacy rights is now a key goal of the Office. Towards this end, a formal evaluation of the public awareness campaign will be carried out during 2005 in the light of an updated public opinion survey of data protection awareness. The last such survey was carried out in late 2002. Furthermore the Office will also, during 2005, launch a specially commissioned training video and accompanying facilitator's work-book which is being designed to act as a stand-alone training product in Data Protection.

INFORMATION FOR DATA SUBJECTS

Data Protection starts and ends with each individual and to this end, people must make sure that they read the Data Protection statement on any forms that they fill out. This should make clear in plain language and with appropriate prominence what is being consented to by data subjects. The bottom-line in data protection law is that there should be openness and transparency and that processing of personal data should entail no surprises for the data subject.

In this regard, section 2D of the Acts (following Articles 10 and 11 of the Directive) specifies the information which should be given to a data subject. The Article 29 Working Party of EU Data Protection Commissioners during the year endorsed the principle that a fair processing notice on websites does not need to be in the same format but could be provided in up to three layers of information as follows:

Level 1 – The short notice

This must offer individuals the core information required under section 2 D of the Acts and Article 10 of the Directive namely, the identity of the controller and the purposes of processing – except when individuals are already aware-and **any additional information which in view of the particular circumstances of the case must be provided beforehand to ensure a fair processing.** In addition, a clear indication must be given as to how the individual can access additional information.

Level 2 – The condensed notice

Individuals must at all times be able to access a notice of information to include all relevant information required under the Acts and Directive. This includes, as appropriate:

- *The name of the company*
- *The purpose of the data processing*
- *The recipients or categories of recipients of the data*
- *Whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply*
- *The possibility of transfer to third parties*
- *The right to access, to rectify and object*
- *Choices available to the individual.*
- *In addition, a point of contact must be given for questions and information on redress mechanisms either within the company itself or details of the nearest data protection agency.*
- *The condensed notice must be made available on-line as well as in hard copy via written or phone request. Data controllers are encouraged to present this notice in a table format that allows for ease of comparison.*

Level 3 – The full notice

This layer must give complete information and cover all legal requirements.

Templates for the short and condensed Privacy Notices are available on the Article 29 website at http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp100_en.pdf . I commend them to data controllers as a model for informing data subjects about processing of their personal data. While these notices are more suitable for online activities they can easily be adapted for offline transactions provided an individual is given a simple means (e.g. a freephone number) to obtain detailed information.

NATIONAL DIRECTORY DATABASE

The Privacy in Electronic Communications Regulations 2003 (S.I. 535 of 2003) set out the rules for recording subscribers indications as to whether they wish to receive unsolicited direct marketing telephone calls. The Commission for Communication Regulation (ComReg) was due to issue an order in July 2004-after significant input from my Office-amending the National Directory Database (NDD) so that it will also become the national telephone marketing opt-out register. When set up, direct marketers will be required to consult this **national 'opt out' register** and the wishes of subscribers must be respected, or otherwise an offence will be committed. I am very disappointed that after such a long period of consultation with the industry, the order amending the NDD had still not been made by ComReg at year end because data subjects were deprived of the means to have their direct marketing preferences respected as allowed by law.

WEBSITE INFORMATION (WWW.DATAPROTECTION.IE)

During 2004, there were many visitors to the site which displays detailed information on Irish data protection legislation and practice as well as providing links to European Union Data Protection Authorities and other privacy sources. By the end of the year, material was updated extensively and the process of redesigning the site to make it more user friendly and incorporating a search engine was commenced.

DIRECT CONTACTS-TALKS AND PRESENTATIONS

During the year, 72 Presentations were made by staff of the Office and myself, to organisations in both the public and private sectors, as well as at Conferences, both in Ireland and abroad. Over 6,000 people in all attended these presentations. Details are given in Appendix 3.

ENQUIRIES

The Office received some 15,000 enquiries whether by personal callers to the Office, phone, email or correspondence. A major focus of the work of all staff involves giving a prompt and informed response to queries which may emanate from individuals, public and private sector organisations, voluntary groups and legal advisors, teachers and citizens advice centres. Enquiries continued to increase, as both Data Controllers and the Public became more aware of their responsibilities and rights. The queries have tended to be more complex, and reflect an interest in the effect of the new legislation.

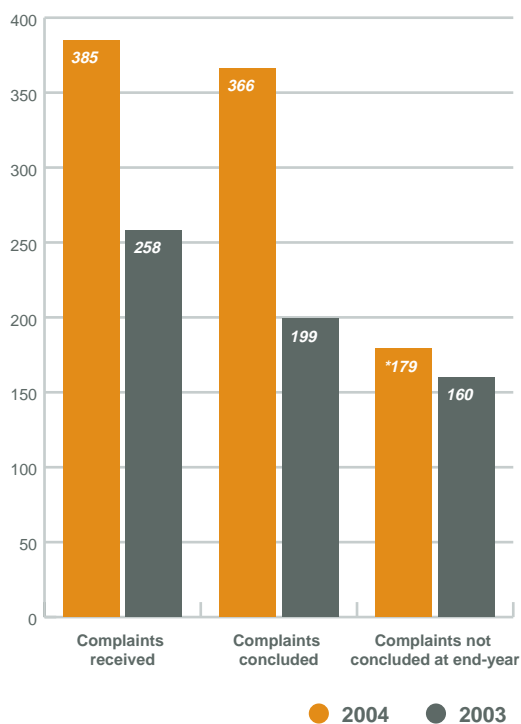
COMPLAINTS AND INVESTIGATIONS

Under the Acts, I may launch an investigation into a 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 otherwise of opinion that there may be a contravention. Where a complaint is received, I, as Commissioner, am required by section 10 of the Data Protection Acts, 1988 and 2003, to investigate it, and, to arrange an amicable resolution. Failing that, I am required to issue a decision in relation to it.

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 is established are required to address shortcomings and put new procedures and practices in place. While I have no power to issue fines in respect of contraventions, I may issue a formal decision which is subject to a right of appeal by either party to the courts. Individuals who have been the subject of a contravention may make a claim for damages in the courts under section 7 of the Acts.

During the year, the increasing complexity of the case-load posed challenges for the staff. During 2004, the number of new complaints processed formally was 385 (of which 131 were in relation to alleged contravention of the Privacy in Electronic Communications Regulations (S.I. No.535 of 2003) by unsolicited direct marketing chiefly on mobile phones) compared with 258 the previous year (and 78 in 1998). The number of complaints concluded was 366 and at year's end 179 were still on hand. This is illustrated in **Figure 1** below.

Figure 1
Complaints received, concluded and not concluded:

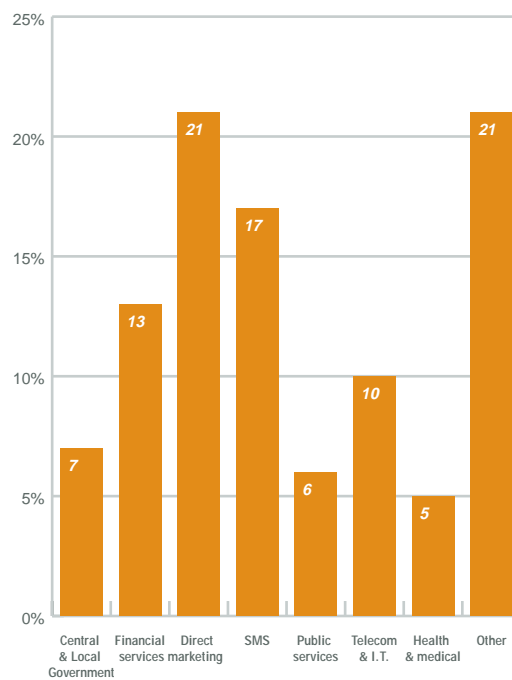


* 179 Complaints not concluded at 31 December (includes 23 received in 2003) comprising

On going inquiry 3
With the data subject 7
With the data controller 75
With the Office for review and further consideration 94

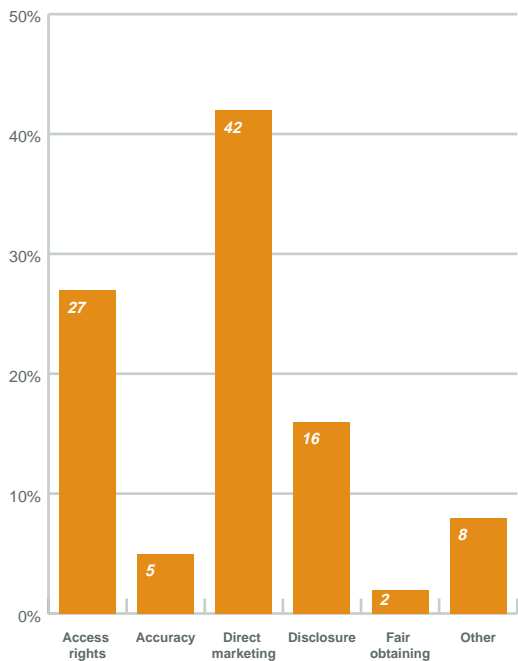
Figure 2 shows a breakdown of the types of organisation against which complaints were made to this Office in 2004. 13 per cent of complaints concerned the financial services sector. The Telecommunications / IT sectors accounted for 10 per cent, while the direct marketing sector accounted for 21 per cent of complaints. The public services and Central and Local Government accounted for 13 per cent of complaints.

Figure 2
Breakdown of data controllers by business sector



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 Act (27%) and complaints about direct marketing (42%). Complaints about the issue of fair obtaining and incompatible disclosures of data to third parties were the next most common issue of complaint (together totaling 18%).

Figure 3
Breakdown of complaints by data protection issue

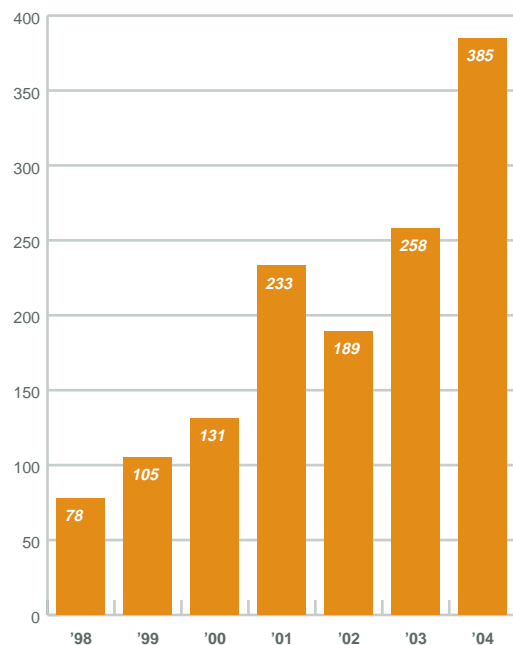


This was the first full year of operation for the Electronic Communications – Data Protection and Privacy Regulations (S.I. 535 of 2003) which *inter alia* provide for the offence of sending unsolicited marketing messages by electronic means, also known as SPAM. Complaints received relating to this issue came to 131. Nearly half of the complaints received related to three marketing campaigns run by two companies. As some of these complaints will result in the taking of prosecutions, they can take longer to resolve.

In addition to the complaints received, I have also been contacted by a large number of people who have subscribed to services – chiefly on mobile phones – and then wish to

complain about the manner in which the services were delivered (typically the recurring charges). This is a matter in which I cannot become involved, as these services ceased to be unsolicited once a person subscribed. It is my advice that people act responsibly when signing up to services such as telephone ringtones. In some instances, the Regulator for Premium Rate Telecommunications Services (RegTel) has been able to assist people unhappy with these services.

Figure 4
Complaints received since 1998



Of the complaints concluded, I found that 26% were upheld, 63% were resolved informally while 11% were rejected. Details of the more significant cases are summarised in the Case Studies section in Part 2 of this Report.

As **figure 4** indicates the increase in complaints since 1998 is very significant.

THE PUBLIC REGISTER

The number of organisations registered with my Office rose by 891 or 19% in 2004. This represents another significant increase, which has been brought about primarily by our focus

on those who are required to register because they process sensitive data. Health Professionals, legal representatives, schools and politicians made up most of the new registrations in 2004. I see registration as a valuable tool in ensuring compliance. It brings those organisations that process significant volumes of personal data or data of a sensitive nature into regular contact with my Office.

In addition to increasing compliance with the registration requirement, my Office has given a high priority to improving the quality of the entries on the register. This happens on an ongoing basis but the Office also organised seminars for three sectors - local government, credit unions and central government in 2004. These seminars covered the updated legislation and also what the Office expects in terms of the register entry. These seminars proved very successful particularly in relation to the local authority registrations

I also made a submission to the Minister for Justice, Equality & Law Reform in response to a consultation process on who will be required to register under regulations to be introduced under Section 16 of the Data Protection (Amendment) Act 2003.

CODES OF PRACTICE

Under the 2003 Act, I have power to prepare and publish "codes of practice" for guidance in applying data protection law to particular areas. These codes, if approved by the Oireachtas, have binding legal effect. During the year, work was continued on Codes of Practice for the Funds Industry and for the Employment area. In regard to the latter, a preliminary step is the adoption by IBEC, following discussion with my Office, of a Data Protection Policy Statement template. I also published Employment related Data Protection Guidance on my website and it will be my intention to have a formal public consultation process in order to move this important matter forward. Case studies 1 to 3 refer to employment related issues. Work is ongoing on finalising drafts for the banking, financial services and insurance sectors as well as the Gardai.

As a means of assisting sectoral organisations in developing Codes of Practice, I intend in

the next year to bring forward a self-audit manual which will help organisations to establish where they are in terms of Data Protection compliance. This will serve as a foundation for the development of Codes of Practice which will add to Data Protection compliance.

PROSECUTIONS

Successful prosecutions were taken in 2004 against two data controllers for not registering with my Office while a prosecution against a third for failure to answer an Information Notice was not proceeded with as the firm registered following the issuing of the summons. In late 2004 my solicitors were instructed to issue summons to 4's a Fortune Ltd for contravention of the Electronic Communications Regulations - Statutory Instrument 535/ 2003.

PRIVACY AUDITS

The Data Protection (Amendment) Act 2003 gives me the power to conduct investigations where I consider it appropriate to ensure compliance and not only where I have received a complaint or consider that a contravention has or will occur. I prefer my role to be a proactive one rather than a reactive one. I use this authority to carry out "privacy audits" with the main objective of raising awareness and assisting the data controller in complying with its obligations. If shortcomings are discovered then a follow-up inspection will normally be carried out before enforcement notices or the like would issue. The audit process begun in 2003 was increased in 2004 and the following organisations were audited:

- *Bank of Ireland*
- *Irish Life and Permanent*
- *Garda Síochána*
- *Offaly County Council*
- *Ticketmaster*
- *BUPA*
- *Iron Mountain - an offsite data storage warehouse*
- *Mortgage Providers*

In general my inspection teams have found that there is a reasonably good awareness of and compliance with data protection principles in the bodies that have been inspected. Issues have also surfaced and recommendations made for change. I would like to mention some positive findings in 2004. The internal audit controls and staff training within An Garda Síochána are, as might be expected, at the higher end of standards to be aimed for. The Garda systems show what is technically possible. When systems were being devised, it is obvious that data protection was an important consideration. This is not as obvious when dealing with private sector bodies that process large volumes of personal data. Building data protection into a system after it has been created is difficult. With that in mind, I strongly advise any organisation that is considering developing a new system that they consider their data protection obligations at the design stage.

My inspection teams have also found some excellent data protection training and awareness documentation in use by various bodies. In particular, I would like to recognise the quality of internal documentation used by Irish Life Assurance Plc.

SIGNIFICANT ADVICE GIVEN DURING THE YEAR

During the year, specific Guidance on a range of Data Protection issues was published on our website. In addition specific issues were addressed in advice given to various organisations and these are detailed in Part 3. I intend to issue guidance on medical research and data protection later this year.

INTERNATIONAL ACTIVITIES

During 2004 my Office staff and I participated in the following international activities -

- *Article 29 Working Party of the EU member states and the EU Commission.*
- *EU Joint Supervisory Bodies comprising Europol, Schengen, Customs Information*

System, Eurodac and Eurojust as well as the related Appeals Committees. I was chairman of the Eurojust supervisory body during the Irish EU presidency.

- *Leading, during the Irish EU Presidency, inspections of the supervision of the Schengen Information System, by the data protection authorities in Austria and the UK.*
- *26th Annual International Conference of Privacy and Data Protection Commissioners in Poland.*
- *Spring Conference of European Data Protection Commissioners in Netherlands.*
- *International Complaints Handling Workshops in the Czech Republic and Sweden.*
- *International Working Group on Data Protection in Telecommunications in Germany.*
- *Annual meeting of the United Kingdom, Irish, Guernsey, Jersey, Cyprus, Malta and the Isle of Man authorities in Jersey.*
- *Meetings in Dublin and Belfast with the United Kingdom Information Commissioner and the assistant commissioner with responsibility for Northern Ireland matters.*

Addressed the following organisations:

- *American Chamber of Commerce to the EU in Brussels*
- *Members of New Media Developments Committee of the German Parliament on their visit to Ireland*
- *INHOPE-Internet Hotline Providers in Austria*
- *United States Department of Commerce Commercial Law Development Programme - e Commerce Policy and Regulation Consultative Irish Tour for officials from the Government of Egypt.*
- *EU Conference on Biometrics at Farmleigh House Dublin as part of Ireland's EU Presidency.*

As Gibraltar is establishing a data protection commissioner's office, the Commissioner designate visited my Office and later in October its chief compliance officer worked for

one week in my Office. Two members of the Bulgarian Customs service also visited my Office to review the Customs Information System operations and had later discussions with the Revenue Commissioners- this was part of the EU TAIEX programme.

European Union Activity

The Office attended all meetings of the Article 29 Working Party, the consultative body comprising the data protection commissioners of the EU member states as well as the EU Commission. The Commissioners of the applicant countries also attended the meetings as observers in early 2004 and we were glad to welcome them as full members from May 2004. The group makes opinions and recommendations on various data protection issues; it tries to have a uniform approach community wide. The Working Party reviewed its operations and published its first strategy statement during the year.

The matter of the USA request for airline passenger data details to be supplied to its authorities- Canada and Australia have also made similar requests- begun in 2003 was a major part of the working party's work. The focus of the Article 29 review was that the measures should be proportionate and with adequate security. Our final position was published in June 2004 where we expressed serious concerns on aspects of the agreement reached between the EU and the USA. While the EU Commission was happy with the final USA agreement - significant modifications were made - the Article 29 Committee had certain reservations. The European Parliament has since initiated proceedings in the European Court of Justice as to the agreement's legality. Discussions are ongoing with the USA, Canada and Australia.

The developments in biometrics and radio frequency identification (RFID- i.e. radio tracking devices on consumer goods) as well as matters concerning transborder flows of data were also considered.

I chaired a working party comprising EU Commission staff, data protection staff from

other EU countries and representatives from VISA Europe and MasterCard Europe which drew up data protection guidelines on payment card fraud prevention databases.

The Office has continued to provide representation at meetings of the Europol, Schengen, Customs, Eurodac and Eurojust supervisory authorities. As chairman of the Eurojust supervisory body during the Irish EU presidency I succeeded in getting agreement to have its rules of procedure adopted and in publishing its first activity report. In general the supervisory authorities are concerned that data protection is not getting adequate attention when security measures are being promulgated by the EU Commission and/or the Council of Ministers and proposals for a dedicated forum with sufficient resources, similar to the Article 29 Committee, were put forward.

Copies of all Opinions adopted at the EU meetings are available through this Office's website.

ADMINISTRATION

Running Costs

The costs of running the Office in 2004 are as set out in **Table 1**.

Table 1

Costs of running the office in 2004

	2003	2004	change
	3	€	
Overall running costs	1,242,960	1,323,676	7%
Receipts	455,539	530,854	17%

A fuller account of receipts and expenditure in 2004 is provided in Appendix 9.

Staffing

The full authorised complement for the Office is 21 and the filling of all of these posts is vital if the Office is to be able to adequately discharge the additional workload which the new Act is generating. At the end of the year there were 2 vacancies and while I appreciate

the pressure on resources in the public service, the filling of these vacancies is necessary if the Office is to continue to develop and provide an important public service in the pro-active way which we are seeking. I wish to acknowledge the continuing positive response of the Department of Justice, Equality and Law Reform and their understanding of our needs in this regard.

Staff and Performance Development

During 2004, the Office submitted the necessary Progress Report to the Justice and Equality Sector Performance Verification Group which assessed the Office's progress in relation to its commitments which had been agreed under its Modernisation Action Plan. The Office also revised and published a new Strategy Statement and Business plan. The significant elements of these plans are:

Customer Service

Giving prompt and accurate advice to personal callers, either in person, by phone or email, is crucial not only to service delivery but to the public image and status of Data Protection. We are following several initiatives to build on our strong customer service ethos, particularly in the areas of delivering services over the internet and at regional level.

Equality

We seek to disseminate and build awareness of Data Protection across all sectors of society and in particular to promote and encourage access to our service for people who may otherwise feel excluded from the world of computers and e-business. Within the Office, staff have availed of parental leave and job sharing and the Office culture is fully supportive of these family friendly initiatives.

Staff Training and Performance Management

In pushing forward with Modernisation, I am firmly of the view that the most important resource is staff. My policy is to provide an environment where every staff member is both given the opportunity and encouraged to develop their full potential and also where they feel included as part of a team. Staff morale and customer service have been

boosted by our move to new accommodation in May 2003. We are constantly engaged in internal training to develop staff expertise in the new legislation and we see PMDS, with its emphasis on clarification of roles and training, and its link to the Business Plan, as making a key contribution to expertise. This is of significant importance as we plan for a successful and effective decentralisation

A Partnership Committee

The Committee play a positive role with our Action Plan. Staff are also encouraged to contribute, updates are circulated after every meeting and staff are invited to attend as observers, for their own development, and for the purposes of transparency.

Efficient use of resources

The additional staff assigned to the Office over the last few years, has enabled more thorough compliance activity, particularly in regard to registration requirements as over 5,000 controllers have now registered (3,000 in 2001) and in clearing complaints. More and more use is also being made of IT to enhance use of resources and to provide a better service level. The introduction of online registration if it is cost beneficial is being considered but this must await the decision of the Minister regarding future registration obligations.

The Performance Verification Group informed me during 2004 that the progress achieved in relation to the Office's commitments warranted the payment of the pay increases due to all grades of staff in the Office. This is above all a tribute to my staff's commitment and I very much appreciate their continued dedication and support during 2004.

Support Services

I finally wish to record my appreciation for the ongoing services provided by the Department's Information Technology personnel and my appreciation of the Department's Finance Division, based in Killarney, which has continued to provide my Office with a vital service in the area of receipts and payments.

Part 2

Case Studies

- 18** Employment - legal privilege and access to medical data
- 20** Workplace bullying
- 21** References and salary details
- 23** Bar Council's in-house legal diary
- 25** Political database and 'spamming'
- 27** Affordable housing and website publication
- 29** Eircom and barring orders
- 30** Planning applications
- 31** Medical research
- 32** Bank of Ireland marketing campaign

Case Study 1

EMPLOYMENT MATTERS – CLAIM OF LEGAL PRIVILEGE AND ACCESS TO MEDICAL DATA IN THE WORKPLACE

An employee of a major national company had been requested to attend a doctor nominated by the employer in the context of his on-going sick leave. His employment was subsequently terminated and he made an access request under section 4 of the Data Protection Acts for a copy of the medical report. The company refused him access on the grounds that the employee had initiated legal proceedings against the company and that the report was privileged and that it did not have to be released as section 5(1) (g) applied. This section provides that the right of access under section 4 of the Acts does not apply to personal data

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



I pointed out that there are two main categories of legal professional privilege recognised by Irish Courts:

Confidential communications between an individual and their lawyer seeking or giving legal advice and documents created by either party to provide or to obtain such advice are privileged.

Documents created by either lawyer or client in anticipation or furtherance of litigation are also privileged. Therefore, communications between an individual and their lawyer which provide legal advice or assistance, and documents created to obtain or produce such advice or assistance, are privileged if given or created in anticipation or furtherance of litigation.

In deciding whether privilege could be claimed, I considered **the purpose** of the referral to the doctor and specifically whether it was in anticipation of legal proceedings or to obtain legal advice or whether the purpose was to determine fitness for work.

The complainant stated that he had been requested by letter to attend the doctor to have his condition assessed due to his on-going sick leave – no reference was made to attendance being requested in connection with any court proceedings. The company however sought to claim to my Office that the report had been sought on legal advice and in anticipation of possible future legal proceedings. I found that while there may indeed have been a possibility of legal proceedings in relation to other matters, the first formal notification of court proceedings was sent by the data subject's solicitors many months later. I further found that **the purpose of the medical examination should be clear to the data subject at the time that he attends the doctor.**

The employee in this case was clearly under the impression that the referral was related to assessing his fitness for work only. It is an important Data Protection principle that **another purpose cannot be introduced retrospectively.** Furthermore, information about the purpose is required to be provided to the employee (data subject) pursuant to section 2(D)(i) and (ii) of the Acts, otherwise personal data is not treated as “fairly processed”.

Privilege is an important feature of court proceedings but it should not be used as a veil to seek to restrict access where it cannot be justified. As section 5(1)(g) relates to personal data in relation to communications between a client and his/her professional legal advisers or between those advisers, I took the view in this case that a copy of a medical report prepared for a specific personnel purpose could not be considered as such a “communication” which would attract privilege. Also, there are very limited restrictions on an individual’s right of access to his or her medical data. The Data Protection (Access Modification)(Health) Regulations, 1989 provide that restrictions on access must be based on opinion by a medical professional that allowing access would cause serious harm to the individual’s physical or mental health. As “harm” was not an issue, I therefore concluded that section 5(1)(g) of the Data Protection Acts, 1988 and 2003 could not be relied upon by the company to restrict his access to a copy of the medical report in question. I was pleased that the company accepted my view.

In another employment related case, I established that a data controller cannot avoid dealing with an access request for an employee’s medical report on the premise that it has been returned to the author of the report. To deal with such requests, organisations should have a clear procedure in place. The request may be for (1) the report itself and/or (2) the data on the medical file. When an access request for medical data is received, the Company Doctor/Medical Officer should be immediately advised and should make the data available unless it is considered ‘harmful’ to do so.

On a related question, it is sometimes considered that the employee’s consent is needed for referral to a company doctor. Generally, an employer will have the right under the contract of employment to refer an employee for a medical report. Processing of personal data in a medical report involves sensitive data and section 2(B)(i) of the Acts provides that a data controller must obtain “**explicit**” consent from a data subject before

Privilege is an important feature of court proceedings but it should not be used as a veil to seek to restrict access where it cannot be justified- generally, an employer will have the right under the contract of employment to refer an employee for a medical report

sensitive data may be processed. Alternatively, section 2B(ii) provides for processing which “**is necessary for the purpose of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.**”

Relying on freely given consent implies that an employee has a right to refuse referral. Given the employer’s rights under the contract of employment, this may not fully reflect the entirety of the rights and obligations involved. Therefore when the employee agrees to attend the doctor, what is important is that the employee clearly understands that s/he is required to attend the medical assessment for a particular purpose e.g. to determine whether s/he is fit to return to work and attends on that basis alone. On the other hand, if the purpose is connected with anticipation of or defence of legal proceedings then the employee should know that this is the basis for the referral.

Case Study 2

WORKPLACE BULLYING AND HARASSMENT

An employee had made an access request under section 4 of the Acts for personal data contained in a human resources division investigation file concerning a bullying and harassment complaint which he had lodged against another member of staff.

The data controller explained to me that the complaint was of a serious nature and that the matters were being investigated under the employer's policy on bullying and harassment in the workplace. They stated the view that until such time as the investigation was completed, documentation prepared in connection with the investigation would, if disclosed at a juncture not provided for in the process itself, be likely to prejudice the effectiveness and fairness of the investigative process and that it is therefore not liable to be disclosed. They confirmed that only



documents prepared in connection with the ongoing investigation were withheld in this manner, on the basis of section 5(1)(a) of the Data Protection Acts which provides that the right of access 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,

I found that the action taken by the data controller in withholding data in relation to the ongoing bullying and harassment investigation was in accordance with the provisions of section 5(1) of the Data Protection Acts. On completion of the investigation, this section however would no longer be applicable.

documentation prepared in connection with the investigation would, if disclosed at a juncture not provided for in the process itself, be likely to prejudice the effectiveness and fairness of the investigative process

Case Study 3

REFERENCES AND SALARY DETAILS DISCLOSED WITHOUT PERMISSION

I received a complaint from an individual who had applied for a specialized medical post with a major hospital. He had forwarded his CV accompanied by a letter in which he stated that he withheld consent to the organisation contacting the referees listed on his CV until “mutual interest” had been established and he had time to appraise the referees of his intentions. He was subsequently contacted by the Human Resources section informing him that they had already contacted the referees.

I took this matter up with the hospital concerned who immediately acknowledged the error and that the individual's wishes had been overlooked by contacting the referees. They said that they had put revised procedures in place to avoid this happening again.

A fundamental principle of the Data Protection Acts is that personal data should not be disclosed to third parties without the data subject's consent or unless one of the exemptions provided in section 8 applies. In the circumstance, I found that contacting referees without consent is a disclosure in contravention of section 2(1)(c)(ii) of the Acts which provides that:

2.-(1) A data controller shall, as respects personal data kept by him or her, comply with the following provisions:

(c) the data-

(ii) shall not be further processed in a manner incompatible with that purpose or those purposes.

(Processing is defined in the Acts to include disclosing data).

In this case, insufficient care appears to have been taken by the organisation to ensure that appropriate guidance was provided to staff involved in the recruitment process and that clear procedures were in place which reflects best data protection practice in regard to the contacting of referees. In my decision, I advised that written consent should be

obtained to have reference enquiries taken up and that this should be exercised only in respect of candidates who are being short listed or to whom a provisional offer is being made.

In another case, the personal data of some 260 employees and former employees of a major financial institution were disclosed to more than 100 prospective job applicants by the institution's recruitment agency. The institution had forwarded a spreadsheet of vacancies and job profiles to the agency and a file was attached inadvertently giving details of people who had filled these jobs. The details were name, role, line manager, details of previous employer, start date, starting salary, previous salary and previous job title. In no way should this information be released. While the recruiting agency had controls in place to ensure that personal data was not disclosed, nevertheless an employee deliberately overwrote those controls when he was having difficulty with the system in order to circulate the spreadsheet expeditiously.

while the agency had controls in place to ensure that personal data was not disclosed, an employee deliberately overwrote those controls when he was having difficulty with the system in order to circulate the spreadsheet expeditiously.

From my enquiries, I was satisfied that the contracts in place between the data controller and the recruitment agency (who were a data processor within the meaning of the Acts) met the requirements of section 2(C) (3) of the Acts which specifies the contractual provisions relating to security measures which ought to be in place between a data controller and data processor.

I also found that section 2(1)(d) of the Acts was contravened in that an unauthorised disclosure in respect of personal data was made inadvertently to certain third parties, as a consequence of persons employed by agents of the controller not complying with the relevant security measures required by section 2(C)(1) and (2) of the Acts.

In my decision, I emphasised that data controllers must make their staff aware of their data protection responsibilities through appropriate training and/or the availability of an internal data protection policy. An internal policy should reflect the eight fundamental data protection rules, which should be enforced through supervision, audit and regular review particularly in terms of constantly reemphasising security awareness amongst staff and management. While such an approach may never give 100 per cent protection against individual human error, it may help to satisfy me in any given case that a data controller has taken reasonable measures to comply with the security requirements of section 2(C)(1) and (2) of the Acts.

As a similar type of incident by another agency was the subject of Case Study 6 in my 2003 Report, recruitment agencies must be extra vigilant and I intend to conduct a review of their data protection systems in the coming years.



consent should be obtained to have reference enquiries taken up and this should be exercised only in respect of candidates who are being short listed or to whom a provisional offer is being made

Case Study 4

THE BAR COUNCIL'S IN-HOUSE LEGAL DIARY AND ASHVILLE MEDIA

The Bar Council complained to me about the use of their members' data by a publication "The Irish Legal Professional", which was published by the Ashville Media Group. The Bar Council explained that Ashville Media Group had published the Bar Council's in-house legal diary, which was for the sole use of barristers from 1998 to 2002, under contract. On expiry of the contract, the Bar Council then changed to another company for publication of the diary. In order to publish the barristers' diary, Ashville Media Group had been afforded access to an internal database containing contact details for all barristers, including their home addresses, home and work telephone numbers, mobile numbers and email addresses. The Bar Council stated that despite the termination of the contract



between the Bar Council and Ashville Media Group, Ashville Media Group used the database in their own publication "The Irish Legal Professional" in 2003 and 2004.

In my investigation, Ashville acknowledged the facts alleged in the complaint. However they submitted that the personal data (contact details) of barristers are already in the public domain and are readily available to the public, and as such the Legal Diary simply makes these more accessible to barristers and solicitors. I noted that section 1(4)(b) of the Acts provides that *the Acts do not apply to personal data which is required to be made available to the public by the person keeping it*. However, I was satisfied that there is no legal obligation on the Bar Council to make the personal data of barristers available to the public so I found that section 1(4) was not relevant in this case. **However, even if it was the case that barristers' details are in the public domain by virtue of a requirement on the Bar Council to publish the data, that would not absolve other data controllers or data processors acquiring those data of their obligations under the Acts.**

In my decision, I noted that during the currency of the contract, Ashville was a data processor on behalf of the Bar Council within the meaning of the Acts (a data processor being a person who processes personal data on behalf of a data controller). I found that this means that **personal data obtained for the purposes of a data processor contract may not be processed subsequently for a different purpose**. Therefore, as a data processor, Ashville in publishing the contact details of Barristers in their 2003 and 2004 Guide, contravened section 21(1) which provides that

"personal data processed by a data processor shall not be disclosed by him...without the prior authority of the data controller on behalf of whom the data are data processed".

I also found that Ashville Media Group

- *in continuing to process the data were in that respect also a data controller and that as such they had contravened section 2(1)(c)(ii) of the Acts by further processing the data for a new purpose, i.e. in publishing the contact details of Barristers in their 2003 and 2004 Guide;*
- *as a data controller, had contravened section 2(1)(a) of the Acts in that the data was not fairly obtained for the new purpose and*
- *contravened section 2A of the Acts in that none of the conditions specified in that section (consent or another specified condition) were met in order to legitimise the processing of the data.*

In reaching my decision, I required Ashville to delete the Bar Council's 2002 database and any other data derived from it i.e. the 2003 and 2004 databases, and I noted that they responded promptly undertaking to comply with this requirement. Accordingly, I decided not to institute proceedings against Ashville Media for an offence under section 21(2) of the Acts.

personal data obtained for the purposes of a data processor contract may not be processed subsequently for a different purpose-responded promptly undertaking to comply with Commissioner's requirements and not necessary to prosecute

Case Study 5

POLITICAL DATABASE AND A CHARITY REQUEST, “SPAMMING” OF CONSTITUENTS AND NON CO-OPERATION FROM A COUNTY COUNCILLOR

During the year, I received two complaints concerning matters relating to political activity which raised important data protection issues.

The first related to a political party. It was alleged by the complainant, a member of this party, that another local member of the party who was also a member of a charitable organisation had sent him a fund-raising letter on behalf of the charity which identified him as “an active member of our community within the party”. He maintained that his contact details were obtained from the party membership list held locally.

While the appeal for the charity was worthwhile nevertheless once a complaint was received I had to take the matter up with the party's national headquarters. It responded promptly and acknowledged that the local member had used the local party database in sending out an appeal for funds for the charity. While the individual was well-intentioned, the headquarters accepted that the use of data in this way was a contravention of section 2 of the Data Protection Acts, 1988 and 2003 which provides that personal data

(i) “ shall have been obtained only for one or more specified , explicit and legitimate purposes”

and

(ii) “shall not be further processed in a manner incompatible with that purpose or those purposes.”

Data relating to membership of a political party is sensitive personal data within the meaning of the Acts and such data controllers are required to ensure that appropriate safeguards against disclosure are in place. This is especially important given the provision in section 2B(1)(x) of the Acts which permits processing of sensitive data without individual consent “*by political parties, or candidates for election to, or holders of, elective political office in the course of electoral activities for*

used the local political party database in sending out an appeal for funds for a charity. While the individual was well-intentioned it was accepted that the use of data in this way was a contravention of the Data Protection Acts.

the purpose of compiling data on people's political opinions...”. In the course of concluding this complaint, my Office advised the party on their obligations as a data controller, particularly in regard to informing members processing personal data of the requirements of data protection.

The second complaint which was received in late 2003 was about an unsolicited email of a political nature which had been sent by a County Councillor, Jon Rainey, of Fingal County Council. It was alleged that in June 2003 he had “harvested” email addresses from the address line of an email sent by a third party – who was also a County Councillor but of another party. (“*Harvesting*” refers to the addition to one's own mailing list of any email address received on the “to” or “cc” line of the email). This was in contravention of the provisions of S.I. No. 535 of 2003 (European Communities (Electronic Communications Networks and Services (Data Protection) Regulations 2003) which provides for prior consent for unsolicited emailing of individuals for direct marketing purposes, including political purposes.

I only name Mr. Rainey in my Report as he failed to cooperate with my investigations and only acknowledged the facts of the complaint 6 months after I had first raised them and then

only when I had to formally issue him with an Information Notice under sections 10 and 12 of the Acts. At that late stage, he confirmed that the details of email addresses “harvested” from another email had been deleted from his system and that no further details had been obtained in this manner. However, his attitude to my Office was that the matter was of little consequence and he complained that I had “pestered” him.

It is important that public representatives and candidates for elective office realise the importance of their obligations under the Acts and that, in so far as responding to legitimate investigations from statutory office holders is concerned, in no sense should they consider themselves above the law. In this case, I was concerned that a public representative failed to see the significance of a complaint that he was “spamming” his constituents and equally that a lot of unnecessary correspondence and time could have been spared if a full reply to this matter had been received initially.

That said, I am pleased to record that this was an isolated incident as any complaints I have received regarding political activities are normally responded to in a proper and prompt manner.

a public representative failed to see the significance of a complaint that he was “spamming” his constituents and equally a lot of unnecessary correspondence and time could have been spared if a full reply to this matter had been received initially - an isolated incident as any complaints I have received regarding political activities are responded to in a proper and prompt manner.

Case Study 6

LAOIS AND FINGAL COUNTY COUNCILS - AFFORDABLE HOUSING, CREDIT CHECKS AND WEBSITE PUBLICATIONS

It came to my attention that Laois County Council were requiring applicants for Council Loans and Affordable Housing to apply to the Irish Credit Bureau for details of their credit histories. The form given to applicants stated:

“The purpose of this form is to enable you to present to the Council details of any borrowings you may have with banks, building Societies or other agencies. It enables the Irish Credit Bureau to run a credit check against your accounts and to verify your current balance.”

This statement was inaccurate, as the Irish Credit Bureau does not hold information on current accounts. I pointed out to the Local Authority and to the Department of the Environment, that my guidelines for the credit referencing sector (published in my Annual Report for 2000) stated that once personal data is stored on a credit referencing database, **it should be used only for bona fide credit referencing purposes in accordance with the consent given by the data subjects**, and not for other purposes, such as assessment of individuals’ financial standing by a local authority. In any event, the data held by the Irish Credit Bureau is solely for the information of and accessible by Irish Credit Bureau members (i.e. financial institutions) while individuals themselves may also seek a copy of their credit history.

I made it clear that while applicants for Council loans **may choose** to disclose to the Council, information which they have obtained from the Irish Credit Bureau regarding their financial position, the Council may not **oblige** them to do so. It is, of course, acceptable for the County Council to request evidence of financial standing from loan applicants, but to oblige them to apply to the Irish Credit Bureau and to provide the results to the Council would be a contravention of the Data Protection Acts. Following my intervention, I was satisfied that Laois County Council had revised their

procedures but in order to avoid a similar situation arising with other local authorities, I brought the matter to the attention of the Department of the Environment.

I also received a complaint about the publication by Fingal County Council on their website of the details of people who purchased houses under the Affordable Housing Scheme. I established that under local authority legislation, in the interests of openness and transparency, Fingal County Council were obliged to make available to the public details of proceedings of the Council, minutes of meetings etc. Section 1(4)(b) of the Data Protection Acts, 1988 and 2003 provides:

“This Act does not apply to-

(b) personal data consisting of information that the person keeping the data is required by law to make available to the public,”

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.

This meant that if details of those who purchased houses under the Affordable Housing / Shared Ownership Scheme are included in Council minutes which are required by law to be made available to the public, then such data are not subject to the Data Protection Acts, 1988 and 2003. However, when I became aware of the concerns of individuals whose personal details were displayed on the Fingal County Council website, I had discussions with the Council who agreed that the personal details of applicants for the Affordable Housing / Shared Ownership scheme would be removed from the website. **This reflects the important principle (published in Case Study 3/03) 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.** However, full details will still be available for public inspection at the Council Offices as is required by legislation. The website will provide general information about the allocation of houses under the Scheme and will draw attention to the fact that full details will still be available for inspection at the Council Offices. I was grateful for the responsible manner in which Fingal County Council addressed my concerns.



Case Study 7

EIRCOM – PROCEDURES FOR ENSURING BARRING ORDERS ARE RESPECTED

I received a complaint about Eircom not respecting a Barring Order that had been granted to a wife against her husband. Though she had changed the telephone account details from his name to her name, he had still been able to contact Eircom and had the access codes for voicemail reset so that he could access her voicemail. Furthermore, on closing the account, the final account had been sent to him at his address rather than hers.

Eircom investigated this complaint **thoroughly** from a data protection perspective. They were not able to establish definitively how the matters complained of arose but accepted that either the estranged husband had the account number himself or perhaps had “spun a plausible story” to Eircom. They acknowledged that if it was the latter then their data protection procedures were not adequate in this instance.

Eircom said that cases involving separation can often pose problems as the person leaving the address may be the named telephone account holder. However, they stressed that the procedures are in place for protecting confidential information and that staff are aware of the company's data protection obligations.

Following my staff's meeting with Eircom on this matter, the company commenced a review of security procedures in their customer – facing call centres. I am advised that this review identified a weakness with regard to transfer of service on foot of a barring order. I am pleased to note that they have adopted a new Procedures Document for dealing with transfer of telephone service particularly in cases of Barring Orders which I am satisfied addresses fully the issues which arose in this complaint. I am grateful for Eircom's considerate response to this complaint, which was a distressing experience for the complainant, and the manner in which they

have revised their procedures which should avoid similar occurrence in the future.

On a general level I reiterate that service-providers operating call-centres need to make sure that they have procedures in place for ensuring that personal data of third parties is not discussed with or disclosed to callers inadvertently.

Though she had changed the telephone account details from his name to her name, he had still been able to contact Eircom and have the access codes for voicemail reset so that he could access her voicemail - Service-providers operating call-centres need to make sure that they have procedures in place for ensuring that personal data of third parties is not discussed with or disclosed to callers inadvertently.

Case Study 8

HOUSING PLANNING APPLICATIONS AND WEBSITE PUBLICATION

I received a complaint about the publication on a local authority website of the details of applicants for Planning Permission. I established that local authorities do not have discretion in relation to the publication of information which is included on a particular planning application. The information must be included on the planning list as set out in the Planning and Development Regulations 2001. The following quotations refer:

“27. (2) A list referred to in sub-article (1) shall indicate in respect of each planning application received during the week to which the list relates-

(a) the name and address of the applicant,”

As planning authorities are obliged by legislation to publish all planning applications with specified details, I concluded that there had not been a contravention of the Data Protection Acts in this instance.

It is worth noting that the Planning Acts also require that the names of objectors and summary of the objection be published. The practice by some authorities has been to scan on to the website a copy of the letters of objection which may include contact details of individuals. I advise Local Authorities that while letters and accompanying names and addresses may be published in the interest of transparency, contact details should be omitted. Individuals making objections should be advised that their letter of objection will be published on the website and thus telephone numbers and email addresses should be omitted.



The practice by some authorities has been to scan on to the website a copy of the letters of objection which may include contact details of individuals... telephone numbers and email address should be omitted

Case Study 9

INADVERTENT DISCLOSURE OF CLIENT DATA BY THE MIDLAND HEALTH BOARD TO A RESEARCH BODY

The Midland Health Board brought to my attention voluntarily that there had been a breach of the Data Protection Acts in that data had been disclosed inadvertently to a research body without the consent of the data subjects concerned. Section 2D(1)(b) of the Data Protection Acts 1988 and 2003 provides that

“Personal data shall not be treated, for the purposes of section 2(1)(a) of the Acts, as processed fairly unless...the data controller ensures, so far as practicable, that the data subject has, is provided with, or has made readily available to him or her...” information relating to recipients or categories of recipients of data.

I advised the Board that this requires that data subjects be informed of proposed disclosures of their data and consent obtained. As sensitive data may have been involved, for which explicit consent to process is needed, I required the Health Board to take the following action:

material disclosed should be returned to the Board and any copies deleted

Health Board compliance Officer to be notified

risk analysis to be carried out to assess causes of the disclosure and to set out a programme of remedial action.

The Board promptly advised me that the data had been returned and destroyed and they also outlined the measures put in place to appraise all personnel involved in research of the safeguards needed. I complimented the Board for their responsible approach to this issue but it does point out the need for greater awareness amongst health service personnel and researchers of the Data Protection rules regarding research.

In a nutshell these are that when personal data is held by a data controller solely for statistical or research purposes, it is exempt (by virtue of

section 2(5)(a) of the Acts) from a number of the normal data protection restrictions. The subjects do not have to be told that it is being used for research, as long as it does not give rise to any distress for them (but I do recommend that people be made aware). However, if it is proposed that personal data be disclosed to a third party outside of the control of the data controller, including doctors working for a hospital who may be carrying out research in another capacity, then there is no alternative to obtaining explicit consent. In view of this and to reduce risks of disclosure of sensitive personal data, data should be anonymised (or pseudonymised) in cases where personal identifiers are not needed for the particular purpose in hand- pseudonymisation involves reverse anonymisation where the true identities are retained in a secure part of the computer system to which access is restricted.

Privacy enhancing technologies have a contribution to make in this area and their use needs to be adopted more widely to facilitate necessary health and social research.

greater awareness amongst health service personnel and medical researchers of the Data Protection rules regarding research is necessary... privacy enforcing technologies have a contribution

Case Study 10

BANK OF IRELAND MARKETING OF 12 AND 13 YEAR OLD SCHOOL CHILDREN

I received a number of complaints during 2003 relating to marketing activity by Bank of Ireland in schools where 12 and 13 year olds had received presentations by Bank staff and were offered the opportunity of opening an account. The complaints centered on the lack of parental consent, details on parents being sought, the procedure by which the teacher confirmed the identity of students and the fact that when an account was closed at the request of a parent, the details were still retained by the Bank for 6 years.

In last year's Annual Report, I referred to section 2A(1) of the Data Protection Acts which state that consent cannot be obtained from a person who, by reason of age, is likely to be unable to appreciate the nature and effect of such consent. **I was pleased to note that before I had to make a determination on the matter during 2004, the Bank changed its policy and now focuses this marketing activity on Transition Year Students and classes which are taking Banking as part of the school curriculum.**

In regard to the form for identifying students, this was necessary in order that the Bank may comply with its anti-money laundering identification obligations pursuant to the Criminal Justice Act, 1994. Following discussions with me, these procedures were revised by Bank of Ireland, and a new application form was introduced for second level students who wish to open a bank account. The revised form specifically provides for the student's consent to this verification and states –

"To enable the Bank to comply with its obligations to establish my identity, I give permission to the Bank to contact my school to verify the accuracy of the information I have given on this form against that supplied to my school. For the benefit of my school, I confirm that my school may act upon this authorisation as if it were specifically addressed to my school."

The revised form makes clear to students that if they wish to open an account, they are authorising their teachers to confirm their identity to Bank of Ireland. The revised form does not request information about the parents of the student. I was satisfied that the new procedures comply with Data Protection requirements in that teachers who confirm the identity of the students for the Bank, will be doing so with the authorisation of individual students who have capacity under the Acts to give consent.

In regard to the retention of data, I was advised that the Bank is obliged under anti-money laundering identification obligations pursuant to the Criminal Justice Act, 1994, to hold account opening documentation for six years, even where any money in the account has been withdrawn and the account is closed. Accordingly, in circumstances where there is a statutory obligation regarding data retention, the provision of the Data Protection Acts specifying that data should not be retained for any longer than necessary for the purpose are set aside.

This issue raised sensitive issues regarding children and their capacity to give consent. Parents, teachers and most of all students should be cautious when faced with any marketing campaigns. The test is whether the young person can reasonably be said to understand the implications of supplying personal data and giving consent.

Parents, teachers and most of all students should be cautious when faced with any marketing campaigns

Part 3

Data

Protection

Guidance

- 34** Speed cameras
- 34** Manual data and access requests
- 35** Patient registers
- 36** Biobanks
- 36** Referral of school class-lists to local Health Boards for immunisation programmes
- 36** Access by local authority members to housing applications

SPEED CAMERAS

The Office was asked for advice by a Government Department on the possible use of speed cameras to help to pursue enforcement strategies relating to motor tax evasion. The advice given was that it was necessary to clearly establish what purposes the Garda Speed Cameras fulfil and under what legislation they operate. At present, it appears that data from these cameras can only be legally used for speeding offences under section 21 of the Road Traffic Act 2002.

If the cameras were to be used for any other purposes, then that should be clearly legislated for – in specific stand-alone legislation- and no longer should the cameras be referred to as “speed cameras”. As Commissioner, I am in favour of all proportionate measures for detecting tax evasion, but there is some concern that this proposal could be the start of a “surveillance” society culture. I wondered if any other uses could later be made of these results viz. for location purposes etc. Accordingly, the matter should be reflected on so as to ensure that function creep would not commence.

ACCESS REQUESTS – MANUAL DATA REASONABLY ACCESSIBLE... DISPROPORTIONATE EFFORT

A data subject has a statutory right of access to his/her personal data under the Data Protection Acts, irrespective of whether the data is already in the possession of the person making the access request. The right is intended to give the data subject control over how personal data about him or her is being used, or at the very least to ensure that data subjects have an awareness of the purpose and the context in which their personal information is being processed. In this way, an individual is in a position to ensure that his/her personal data is being fairly processed in accordance with the Acts. The right of access is to personal data and not documents, so the data must relate in a specific way to the individual - the appearance of a name on a page does not automatically render that information personal data. Section 4 (9) provides that

“The obligation imposed by subsection (1) (a) (iii) of this section shall be complied with by supplying the data subject with a copy of the information concerned in permanent form unless-

(a) the supply of such a copy is not possible or would involve disproportionate effort, or

(b) the data subject agrees otherwise.”

As Commissioner I have not defined “disproportionate effort” and am reluctant to do so given my obligation to uphold data subject’s rights. However, I would be sympathetic to a case being made that providing many hundreds or thousands of pages of documentation involves disproportionate effort where most of the documentation has already been supplied. This is so especially in the light of section 4(3) which obliges an individual making a request *“to supply the data controller concerned with such information as he may reasonably require in order ... to locate any relevant personal data or information”*.

It is clear that the entirety of a file may be readily accessible but that “specific information” in the file relating to the particular individual may not be. My view is that data in a manual file organised in chronological order is certainly readily accessible if the date of the data is indicated - if the date is not indicated, specific data may still be readily accessible if the file is small. Accordingly, it is considered that it is legitimate for a data controller to ask an individual making an access request to specify the data being sought by date or other reference in order to render it “readily accessible”. While a data subject has a right to all of his/her data, the provisions regarding “disproportionate effort” and readily accessible data give the data controller scope to address the request in a manner which balances the individual’s rights with the administrative and other costs involved, taking particular account of the need to give access to data that relate to decisions about the individual so that the individual can ensure the accuracy of his/her data.

PATIENT REGISTERS

It is often stated to the Office by medical professionals and others that in the case of some diseases, it is essential for patient treatment, follow - up and service-management that databases/registers are 100 per cent comprehensive in terms of patient coverage. The Data Protection Acts 1988 and 2003 (section 2B (1) (b)) require explicit consent for the processing of sensitive data. This Office’s approach to the context in which such consent is given is that what is important is that the patient is given sufficient information to give an informed consent - the fact of presenting for treatment with full information can normally be taken to imply consent to the associated necessary processing of personal data. The purpose of the register and why it is essential for all patients in their interests to be recorded on it should be explained.

If it is felt that recording on the database is an essential aspect of the treatment and management process, then our approach is that consent to treatment should incorporate consent to going on the database as this is necessary for patient management and follow-up in the patient’s interest (and therefore can be looked upon as part of the treatment process). On the other hand, it may be the case that the recording on the register/database is optional - if this is so, it is appropriate to obtain a separate consent. Either way, full information should be given to the patient about the processing.

The Office is very keen to promote Privacy Enhancing Technologies and the use of anonymisation and pseudonymisation (i.e. reversible anonymisation) where possible and we advocate that such approaches be used in all cases where personal identifiers are not needed for the particular purpose in hand.

In addition, the office advised that Researchers should only have access to anonymised data;

The identifier “keys” should be stored on a separate database - the consultant, should hold these and they should not be available to researchers;

The register should be password protected and sufficient security measures should be in place to protect the sensitive data in the register.

BIOBANK

During the year, I was consulted by the Coombe Womens' Hospital who wished to establish a biobank, using blood donated from the mother at the ante-natal stage, blood from the placenta at pre-birth stage and from the baby's umbilical cord (which would otherwise be discarded). The Hospital wished to proceed on the basis of informed and signed consent and be completely up front and transparent.

Advice was given on the procedures to obtain consent and regarding security safeguards in relation to both the donated tissue and the personal data. Consent will be obtained at the first consultation with the Midwife - a Patient Information Leaflet will explain that the proposed biobank is to enable research which will be of benefit to future mothers. A mother will have the opportunity to later withdraw the consent if necessary. All samples are given a unique project number and stored in a secure biological resource bank. A name will never be used on any information relating to the donated samples. The samples will be **anonymous** (i.e. nobody will know who the donor is), and they may only be used for research projects that have the prior approval of the Ethics Committee of the Coombe Women's Hospital, and the Board of Trustees of the Biological Resource Bank. This Office considered that a most important point was that the link between the patient record and the anonymised research file must be hidden. The importance of security and access restrictions were also emphasised and it was suggested that there be external independent oversight of the database every 2 years.

I welcomed the overall approach being adopted, the desirability of the hospital to be data protection compliant at all stages and I look forward to further discussions on the practical operations of the Biobank.

REFERRAL OF SCHOOL CLASS-LISTS TO LOCAL HEALTH BOARDS FOR IMMUNISATION PROGRAMMES

The issue of school class-lists being disclosed to local Health Boards in connection with immunizations programmes was raised. I advised that School Principals as data controllers have responsibility under the Data Protection Acts 1988 and 2003 for compliance with the Acts. The Acts prescribe that generally data should only be disclosed if one of the exemptions in section 8 applied or if the disclosure could be considered to be a compatible disclosure. One such exemption is section 8(e) which provides that personal data may be disclosed if required by law. However, my understanding was that there is no statutory obligation on Principals to make the childrens' data available to Health Boards. Nevertheless, the importance of School Class Lists being available to the school medical team for follow-up to ensure the protection of childrens' future health, and indeed wider public health, was appreciated and I noted that there is no other fully reliable method of obtaining the Class Lists. I therefore found that the disclosure of data for the purpose of facilitating the immunisation programme could be considered to be compatible with the purposes for which data is collected and held by schools. It was also covered by section 2A(1)(c)(iv) of the Acts which provides for processing (including disclosures) which is necessary

"(iv) for the performance of any function of a public nature performed in the public interest by a person".

ACCESS BY LOCAL AUTHORITY ELECTED MEMBERS TO HOUSING APPLICATIONS

I received an inquiry from a local authority concerning its disclosure to elected members on an annual basis of personal details of applicants for housing. The inquiry arose following one of the presentations my Office made about data protection requirements.

The Data Protection Acts 1988 and 2003 provide at section 2(1)(c)(ii) that personal data “shall not be further processed in a manner incompatible with that purpose or those purposes” for which it was collected.

Compatibility is determined by the connection and foreseen ability of the additional purpose - to be compatible, the new purpose should be a linked purpose which would not cause surprise to a reasonable data subject. From the information supplied, it would be difficult to see how disclosure to elected members of the names and addresses of all applicants for housing in the county is compatible with the purpose for which applicants gave their details. I accept that members have a democratic function but their oversight of the housing process may be capable of being discharged by the supply of anonymised and aggregate data.

Section 8 of the Acts lifts the restrictions on disclosure, in defined circumstances, which otherwise apply under the legislation. This section provides *inter alia* that any restrictions on the processing of personal data do not apply if the processing is-

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

made at the request or with the consent of the data subject or a person acting on his behalf.

As it was not apparent that any of these provisions could be relied on to support disclosure of the personal data of applicants for housing to the elected members I considered that it would not be in line with the requirements of the Acts to continue the policy as operated in this local authority.

Appendices

- 39 Appendix 1 – Freedom of Information and data protection
- 41 Appendix 2 – Political marketing
- 43 Appendix 3 – Presentations and talks
- 45 Appendix 4 – Public Service card
- 48 Appendix 5 – Biometrics
- 51 Appendix 6 – SPAM
- 52 Appendix 7 – Privacy Statements
- 54 Appendix 8 – Registrations
- 55 Appendix 9 – Receipts and payments

FREEDOM OF INFORMATION AND DATA PROTECTION

Freedom of Information (FOI) has a vital role in ensuring transparency in the public service- FOI does not apply in the private sector. There can on occasions be a lack of appreciation of the respective roles of Freedom of Information and Data Protection.

In short Data Protection

Is a human right

Applies to all sectors

Focuses on privacy of one's personal data only

Right of access

computer files initially but since 2003 applies to manual files also

strong with certain exceptions.

while Freedom of Information

Is a citizen's right

Public sector only applicability

Focuses on openness and transparency of both personal and non-personal information

Right of access

all files from the start

strong but refined.

While personal and non personal information are covered by FOI, section 28 of the FOI Acts provides for an exemption in respect of personal data disclosure to third parties if this is deemed to be in the public interest. There is no such provision in the Data Protection Acts. (FOI applies to deceased persons also whereas data protection only applies to living individuals). The Information Commissioner and her predecessors have indicated that the public interest provision is tightly drawn.

In many countries an FOI request for personal information is legally treated as a data protection matter but the Irish legislation only provides that both Offices cooperate. Accordingly, a public sector organisation may get requests under both Acts for access to

personal information and in this regard the Department of Finance is publishing guidance for dealing with this issue. I am pleased to record that cooperation with the Information Commissioner and my Office is good.

The question arises therefore whether FOI could erode a person's right to privacy and whether the release of information under FOI would breach data protection legislation. The Data Protection Acts provide *inter alia* that personal information can be disclosed if it is required by or under any enactment or by a rule of law or by a court order. While this may appear to give *carte blanche* for full public interest disclosure under the FOI Acts exemptions, a European Court of Justice ruling in May 2003 is of relevance.

In this case questions were raised in proceedings between the Austrian National Audit Office and a large number of bodies subject to its control and also two employees of a public broadcasting organisation. At issue was the obligation of public bodies subject to control by the Audit Office to communicate to it the salaries and pensions exceeding a certain level paid by them to their employees and pensioners together with the names of the recipients, for the purpose of drawing up an annual report to be transmitted to the lower and upper chambers of the Federal Parliament and the provincial assemblies and made available to the general public.

The European Court was asked to rule whether such publication contravened Articles 6 and 7 of the EU Data Protection Directive 95/46 – this Directive was transposed into Irish law by the Data Protection (Amendment) Act 2003. Article 6 provides that

Member States shall provide that personal data must be:

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

while Article 7 provides that

Member States shall provide that personal data may be processed only if:

(c) processing is necessary for compliance with a legal obligation to which the controller is subject, or

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed.

The European Court of Justice held that

Articles 6(1)(c) and 7(c) and (e) of Directive 95/46/EC do not preclude national legislation such as that at issue in the main proceedings, provided that it is shown that the wide disclosure not merely of the amounts of the annual income above a certain threshold of persons employed by the bodies subject to control by the Audit Body but also of the names of the recipients of that income is necessary for and appropriate to the objective of proper management of public funds pursued by the legislature, that being for the national courts to ascertain.

Articles 6(1)(c) and 7(c) and (e) of the Directive are directly applicable, in that they may be relied on by an individual before the national courts to oust the application of rules of national law which are contrary to those provisions.

No doubt the Court's ruling will in time be considered by the Irish Courts in particular cases.

Appendix 2

Does political marketing pose special problems for data protection?

Extract from a presentation made by Joe Meade, Data Protection Commissioner, to the September 2004 International Privacy Conference in Wroclaw, Poland.

GENERAL COMMENT

I recognise and accept that the need for candidates in an election or public representatives in the course of their work to contact as many potential voters as possible is fundamental to the proper operation of the democratic process. However such contacts must be made in accordance with legal requirements. In considering this topic the following matters must be considered and a full appreciation of realities of political life has to be understood as well.

POLITICAL ACTIVITY OVERALL

The following are important matters to be taken into account when considering political marketing and data protection as politicians have

An important role and a difficult life as security of tenure is not great

To inform the electorate and freedom of expression is essential.

As democracy demands that people are fully informed by all candidates why put 'barriers' in the way?

Should Data Protection law apply to political activity?

Politicians are processing personal data including sensitive data. Marketing campaigns may be intrusive and why treat political activity as a special exemption? Direct marketing was and is an irritant in the Data Protection area. Therefore Data Protection law must apply.

Is Data Protection law a barrier to political marketing?

We must consider what is legally allowed and the nature of complaints received. It must be

considered whether politicians can be treated differently and in this context the question to ask is - how responsible are politicians or candidates in the manner in which they handle personal data? Therefore data protection law is an enabler overall as it provides a framework within which they can work.

Is political canvassing direct marketing?

When you consider

Recommendation R(85)20 of the Council of Europe

F.E.D.M.A. (1998)

Recital 30 of 95/46 EC Directive

My decision 4/2002 in Ireland

then the answer is yes.

Can politicians direct market and how to do it legitimately?

Yes by adhering to:

Register of electors, as in Ireland politicians have a legal right to have access to it and to use it for political purposes

Direct mailing exemption in Irish Data Protection Acts

EU Communications Directive 2002/58.

What are peoples DP misconceptions in this area?

The following misconceptions arise:

Politicians should not contact me ever

Why have they got my details and where did they get them?

I do not like the message so you must prevent it

It is not right that they can direct market me by using the electoral register when the DPC prevented its use for commercial purposes

How can a DPC be independent when dealing with politicians?

Are there DP special problem areas for political activity?

The following can cause problems:

Automated dialling and recorded message

Automated faxes

Adhere to phone 'opt out' register

SMS texting

Harvesting of email addresses

Using charitable databases to deliver a political message

Individual member not adhering to party policy

How to deal with complaints about political marketing?

The following steps must be taken

Investigate as a normal complaint and assemble all facts

Issue draft decision to Parliamentarians and complainants

Consider responses

Meet with parties and outline basis in detail

Consider their concerns re publicity

Note any mitigating factors

Issue the decision

Prepare for an appeal.

In effect treat as any normal complaint.

If no complaint received

Matter may come to notice in a variety of ways - media, personal contact, opposition party, whatever and indeed the Data Protection Commissioner can initiate procedure on his own initiative if considered necessary. Thereafter treat as a normal complaint problem.

If matter needs to be dealt with urgently then do so. Make sure that you are clear as to purpose of investigation

Special factors in dealing with a complaint

These must not be overlooked

It may be sensitive and diplomacy is necessary

Explore all angles but do not compromise on principles

Be sure to act independently

Outcome the same as for an ordinary complaint by anybody.

CONCLUSION

This is an important area because:

Political marketing creates unique data protection considerations

Demands of political life need consideration

Pragmatic and sensible approach is best.

It is reasonable to assume that the area will present challenges in future.

Appendix 3

Presentations and talks

During 2004 my Office staff and I gave presentations to the following agencies

CARE AGENCY

Homeless Agency

CITIZENS' ADVICE

Comhairle – Dublin, Navan & Longford

COMMERCIAL

Diageo Ireland

COMMUNICATIONS

Regtel

EDUCATIONAL AGENCIES

City of Dublin VEC

Galway Mayo Institute of Technology

HEAnet annual conference

National Centre for Guidance in Education

FINANCIAL SERVICES

*Association of Compliance Officers-
Financial Services- in Ireland*

*Central Bank and Financial Services
Authority of Ireland*

Credit Unions

*Institute of Chartered Accountants of
Ireland*

PWC - Operational Risk Forum

GARDA SÍOCHÁNA TRAINING COLLEGE

Two Superintendents' management courses

GOVERNMENT AGENCIES

Department of Education and Science

Information Society Commission

Labour Relations Commission

Office of the Attorney General

Revenue Commissioners

Customs

*General seminars for Government
Departments*

HEALTH SECTOR

Blackrock Clinic

East Coast Area Health Board

GPIT and Health Boards Conference

Health Informatics Course, Trinity College

*Irish Health Care Risk Management
Association*

Irish Society of Occupational Medicine

Mater Private Hospital

Midland Health Board

National Maternity Hospital

Northern Area Health Board

South Western Area Health Board

*The Irish Society of Hearing Aid
Audiologists*

*University College Cork - Health Summer
School*

Western Health Board

INSURANCE SECTOR

Brokers Federation of Ireland
Friends First Life Assurance Company Ltd

INFORMATION TECHNOLOGY AREA

American Society for Industrial Security
Irish Computer Society at ICT Expo 2004
Irish Electronic Security Forum
EuroKom

INTERNATIONAL

American Chamber of Commerce to the EU in Brussels
Members of New Media Developments Committee of German Parliament
INHOPE-Internet Hotline Providers
Annual International Data Protection Conference Poland
TAIEX-International Customs Cooperation
United States Department of Commerce Commercial Law Development Programme - e Commerce Policy and Regulation Consultative Tour for officials from the Government of Egypt
Complaints Workshop Prague

LEGAL SECTOR

64 Group (Group of legal professionals)
Group of legal professionals on employment aspects
Hayes Solicitors
Law Society-members
Law Society-Protecting Privacy Conference

LOCAL AUTHORITIES

General seminar for all local authorities

MIXED SEMINARS

Cork City for local authority, university and business interests
IIR -National Conference

STATE AGENCIES

Institute of Public Administration
National Disability Authority
Shannon Development
Waterford County Archive Service

VOLUNTARY AND CHARITABLE ORGANISATIONS

Irish Council for Social Housing
National Network of Women's Refuges and Support Services
National Federation of Voluntary Bodies
The Centre for the Care of Survivors of Torture

The presentations in Ireland were made in Counties Clare (1), Cork (2), Dublin (49), Galway (3), Kildare (2), Limerick (2), Meath (1), Offaly (1), Tipperary (3), Wicklow (1) and Waterford (1) with 4 other presentations in Brussels, Salzburg, Prague and Wroclaw. Overall 72 presentations were made to some 6,500 people.

Extracts from a presentation made by the Commissioner in November 2004 to the working party set up to consider the introduction of a public service card-‘SAFE (Standard Authentication Framework Environment) project’

GENERAL

The Government approved in June 2004 the establishment of a top level group to report to Government on the development of a standardised framework for a Public Service card, using the Personal Public Service number as a unique identifier. The aim was said to be the development of a standard for Public Service Cards that would act as a key for access to services, identifying and authenticating individuals as appropriate and where required. It would facilitate over time the convergence of existing cards under a single branded scheme.

Constructive dialogue has started with the Office of the Data Protection Commissioner (ODPC) on this matter. Guidelines on data sharing were published in my Annual Report for 2000 in respect of the REACH initiative. The SAFE project is a big venture and has to be got right from the start. Adherence to Data Protection will enhance and facilitate the delivery of a better service ultimately. It will be important not to overlook other matters - passports, visas, PNR data, USA legislation, UK identity card - which may impact on this work

SCOPE OF PROGRAMME

The Framework approach being adopted seeks to develop standards, capability and infrastructure and is said not to be concerned with the end-uses of the card/token. However to solely focus, from a data protection viewpoint on the SAFE programme is not realistic. You must consider identity management; address the public and private uses as well as the whole area of e-Government. PPSN is ‘classed’ as a national-id number by some academics. Therefore this

project is a major issue for both government and citizens.

WHAT IS OBJECTIVE OF DATA PROTECTION COMMISSIONER?

To ensure that the processing of personal data by Government agencies adheres to the rules in the Data Protection Acts while at the same time having an efficient public service

To ensure that privacy matters are not eroded in the ‘guise’ of efficient services and to have transparent and open practices so as to avoid ‘function’ creep and a national-id number by the ‘backdoor’.

To have stand alone legislation for these developments and not a section in a minor or routine act

CONCERNS TO BE ALLAYED

The lack of real public debate so far on the direction of the Identity Management Framework must be addressed.

What are the conditions or controls that will ensure that the use of the card and PPS number will not lead to contraventions of DP rights? (Up to each organisation but...)

- *Common travel area usage perhaps- what does that mean?*
- *Will Biometrics be included in the card?*
- *Security procedures must be adequate and demonstrated as such.*
- *Are Private sector uses envisaged- Insurance, Banks, Private Health sector?*

FOCUS OF SAFE PROGRAMME

The approach may be to focus on standards of interoperability for a card/token and not be concerned with identity management – on the basis that whatever standards emerge will operate within the identity management framework, on which a policy document is being worked on by CMOD (Department of Finance Centre for Management and Organisation Development) at present. I would have concerns about this approach – I see the question of a card/token and identity management in the public sector as being two sides of the same coin. These must be addressed together.

DIRECTION AND LACK OF DEBATE

There has been a gradual expansion of the permitted uses of PPSN since its introduction by annual amendments to the Social Welfare Act. The SAFE framework will provide for extension of uses beyond those that are currently provided for in legislation. Is direction of Identity Management and card being dictated by infrastructural considerations or points of principle?

NECESSITY FOR CONTROLS

Data protection does not preclude a national identifier or better facilities for electronic sharing but this must be legislated for and greater capability must be balanced with controls.

Directive 95/46 provides that “Member States must determine conditions for operation of a national identifier”

The combination of new e-gov initiatives, proposals and legislative amendments require a much greater appreciation of Data Protection if the principles are to be adhered to as they entail greater power and more complexity e.g.

- *E-govt and in particular IAMS (Inter Agency Messaging System)*
- *Public Services Cards and their use*
- *Extension of use of PPSN*
- *Identity Management*

SHARING DATA

Sharing is or will be facilitated to a greater extent by the technical infrastructure that will be in place for e-government. Is there a danger that priority in the initial stages will be to get buy-in to this infrastructure and to get technical issues ironed out? Ensuring that data is used only for a legitimate or compatible purpose may not be high on the agenda.

How do you ensure that a multiplicity of agencies submitting and taking information from the IAMS (*Inter Agency Messaging System*) are doing so for legitimate or compatible purposes?

SPECIFIED LEGITIMATE PURPOSE

These must be considered in detail and clearly stated in an open and transparent way.

SECURITY

The following concerns have to be addressed

- *PPSN safety- its your number- Is it compromised by wider usage?*
- *PRTB and PPSN on electoral e-register ideas*
- *Identity Theft precautions*
- *Access to information on card on a “need to know” basis*
- *Security features of card*
- *Will card hold sensitive data within meaning of DP Acts?*
- *Who will be the data controller or will there be separate cards -chemist, revenue, gardai, Department of Social and Family affairs, Schengen??*

RIGHT TO BE INFORMED

The business side of organisation has to tell the individual the **purposes** for which data will be processed and to whom it will be **disclosed**. This will require an understanding of the workings of the IAMS etc and being able to specify the restrictions that are required.

Receiving organisations have to understand the limits on the use of the data while the individual must know what information s/he is giving when presenting the card. Will delivery of public services be obligatory on use of card or will other methods be relied on also?

ACCESS RIGHT

Is extra data being held about the location and time of transaction that an individual could choose to access? Informing the individual of the source of the data in response to an access request?

REFLECTIONS

Just because something is technically feasible does not mean that it is good or correct for society overall. We must move with care and caution. Security forces and governments have to be vigilant when considering initiatives which impact on privacy. Some EU states have national ID cards but these are balanced by adequate legislative provisions with privacy safeguards. If we are being asked to sacrifice our privacy we must have details about what we get in return because once privacy rights are surrendered they may be hard to recover. We should therefore surrender these rights reluctantly, on the basis of convincing arguments and facts about other interests of society

RECOMMENDATIONS

The following need to be considered in detail

- *Is it for public services only or for other purposes?*
- *Establish the principles that will underpin the use of the PPS Number and card going forward.*
- *Specify the totality of purposes for which the card will be used or could be used.*
- *Specify the organisations that can process, the type of data that will be stored on the card and the controls that will be in place to ensure that DP rights are respected*
- *Have separate legislation for this area preceded by full public informed debate*
- *Be upfront from the start and determine what you want the card to do for you- too easy to create the card and then add to it piecemeal*
- *ODPC will play a constructive role but that is predicated on openness from all sides.*

Finally the ODPC wants the project to be successful.

Appendix 5

EU Conference on Biometrics

EU CONFERENCE ON BIOMETRICS AT FARMLEIGH HOUSE DUBLIN ON JUNE 14TH 2004 - Statement by Joe Meade, Irish Data Protection Commissioner

GENERAL

Firstly may I thank the European Biometrics Forum and Minister Dermot Ahern for organizing this summit and for the opportunity given to me to speak on this important topic today. Data Protection Authorities and Privacy advocates constantly consider improved means of helping protect the privacy of individuals – Biometrics is personal data and after all personal privacy is a human right. The EU Data Protection Directive 95/46/EC imposes an obligation on persons processing personal data to ensure that data are processed in a lawful manner and Article 17 specifically requires that appropriate technical measures are taken to prevent unauthorised access to, or disclosure of, personal data.

ROLE OF DATA PROTECTION COMMISSIONER

As the Data Protection Commissioner for Ireland let me repeat to this distinguished gathering that I will always be supportive of measures that are demonstrably necessary to protect against crime, terrorism, damage to business assets and /or to improve access controls, but such measures must be proportionate and have regard to the human right to privacy. Data Protection Commissioners are not “luddites” but they do wonder on occasions if a sledge hammer is being proposed to crack a nut. Data Protection law by its nature is balanced legislation, it is not absolute and poses no problems for responsible people and organizations. As a creature of law I am tasked *inter alia* with ensuring that data controllers live up to their statutory obligations under section 2 of the Data Protection Acts 1988 and 2003. These obligations include that of having the safeguards referred to in Article 17 of 95/46. For the safeguards to be compliant with

legislation – and indeed as a good business practice- it is necessary to have regard to

- *The state of technological development*
- *The cost of implementing security measures*
- *The nature of the personal data*
- *The harm that might result if such personal data were unlawfully processed.*

In common with other Data Protection Authorities, I am constantly looking for the best means of protecting personal data in an effective and non intrusive manner. However, I am reluctant to accept such solutions at face value. I am fully aware that it is in the interests of many to promote the concept that if technology is the problem, technology can be the solution. Buzzwords such as Privacy Enhancing Technologies, or indeed Biometrics, can be very appealing and may seem to offer a satisfactory solution. An over reliance on technology is not a healthy thing. The easy solution, however tempting, need not necessarily be the most desirable one. But technology is not the problem; technology is neutral, in itself neither good nor bad. It is the motivation with which people employ technology that renders it good or bad. **This should never be lost sight of.**

My sole motivation is to protect a fundamental human right to privacy guaranteed in Irish and International law. In ensuring that right is respected, I will examine all means, products or services at my disposal.

REQUIREMENTS TO SATISFY DATA PROTECTION LAWS

But I must judge whether by employing, or encouraging the employment, of such, I shall be doing more harm than good. It is with this in mind that I must assess whether biometric technology poses a threat to the privacy rights of individuals or whether it is a useful tool to employ to defend those rights.

Before making such assessment, I must examine a number of aspects of the technology:

- *What is its purpose?*
- *Can it reasonably achieve this purpose?*
- *Is it proportionate?*
- *Will reliance upon this technology create a threat to privacy rights?*

The purpose of biometrics is to offer a means of identification or verification and thus, amongst other things, to **assist** in ensuring that only an authorized person has access to specific personal data. This purpose certainly has data protection appeal, but does it work?

There are two principal means by which a biometric can be employed: either a reader at a point verifies that a person's biometric (fingerprint, iris scan, face) matches that held on the card, a so called authentication/verification system, or a reader at a point checks that person's biometric with a central database, a so called identification system.

The first of these is the more appealing in data protection terms, as it does not involve any data being held on a central database. Data are processed purely to create a biometric chip on a document and then check it thereafter. All this is done in the presence of, and to a degree under the control of, the data subject. This degree of transparency satisfies a fundamental principle of fair obtaining and processing. The weakness of this system lies in the security on the identity document. It will be very tempting for those with criminal intent to try to decrypt the biometric chip, to replace the owner's biometric with a false one and to assume another person's identity. Time will tell how common this becomes and whether, like credit card cloning, society will tolerate a certain level before becoming concerned.

The second means of using a biometric relies upon a central database. This raises more data protection concerns. The first one is identifying whether there is a need for such a database. If there is no need to hold the data, then the data should not be retained. However, if the need can be demonstrated, and it is clear as regards purpose and proportionality, then the next concern is about the potential

secondary uses of the database. There must be proper assessment of this risk and restrictions placed on such secondary uses, which may well have administrative or business advantages but which will involve "leakage" and 'function' creep beyond the originally stated purpose. Adequate safeguards must be put in place to prevent processing for any other purpose.

Another concern might seem more appropriate to the realm of Hollywood, but a centralised database will be a tempting target for anyone trying to assume another person's identity. The more biometrics becomes a feature of everyday life, the greater that temptation shall be. Industry may reassure us that a failed check on a biometric (possibly in the order of up to 10%) will only result in the user being required to undergo a manual check to confirm his/her identity. That might work at a border control, though made more difficult if a central database has been compromised, but how will it work when your ATM swallows your card on a wet Friday night and you have to walk home?

That may seem fanciful and exaggerated, but I think it helps make the point that it would be foolish and dangerous **to rely solely** upon biometrics as a means of identification.

THREAT OR OPPORTUNITY

I asked the question if reliance on biometrics would pose a threat to privacy. I think that you can all agree that over-reliance would certainly pose a threat and that this threat is greatest where a central database exists. It is of course easy to accept the apparent need for central databases for law enforcement purposes and to see the appeal for inclusion of some form of biometric in the Schengen or Visa Information Systems at European level. But identifying the need to have a database is essential, as before long leakage occurs- function creep starts- from State to commercial sectors, with biometrics being used for financial transactions, by utility companies or service providers, or by pizza delivery companies. And I'm not even going to begin to talk about

the prospect of third countries with poor national data protection legislation accessing our national databases.

Thus confidence and trust become important factors in determining if biometrics are the way of the future. To build trust it is essential to be certain that personal data held in biometric form are accurate; that the data are held in a secure manner and that the purposes in processing data are known to the data subject. This adherence to data protection principles will demonstrate a respect for privacy and help build the public confidence necessary for biometrics to become accepted. Any doubts generated about the respect for privacy may result in biometrics going the way e-voting evolved in Ireland.

There is one final concern I'd like to mention. Whilst most of my European colleagues live in countries that either have a national identity number, or are considering introducing one, according to the Minister for Justice, Equality and Law Reform, this country has no such plans. However, the use of the same biometric on official as well as commercial identity cards will effectively create a national identifier in the form of a biometric, a biometric as an identity management tool. Whilst the creation of a national identifier is a matter for Government and the Oireachtas, the possibility of the introduction of one through the "backdoor" should not be ignored.*

CONCLUSION

I hope now, given the above, we can embark upon an informed debate about the future of biometrics. To get the ball rolling, I'd like you to think about two things:

Will the use of biometrics add significantly to the accuracy or security of existing verification or identification systems, or is it a further means of intruding on our private lives in the guise of enhanced security?

What is driving the biometrics agenda and has the cost benefit of its effectiveness been published and debated in detail as to its overall reliability?

** In January 2005, the Minister for Justice Equality and Law Reform signalled the need to have a national debate on the issue of a National Identity Card.*

Appendix 6

SPAM initiative

It is acknowledged that to tackle the international problem of SPAM, a combination of technical, legal and educational measures are required and there has to be international co-operation between the various authorities responsible for tackling this issue. My Office participates in meetings of a group made up of EU enforcement authorities which are drawn from the Consumer Protection, Telecommunications Regulation or Data Protection depending on where the responsibility for SPAM enforcement lies. This group has recently agreed on a procedure for co-operation on investigations that involve more than one EU country.

My Office has also signed up to the London Action Plan which provides for co-operation and the sharing of experience and knowledge beyond the EU and with private sector organisations.



Appendix 7

Absence of Privacy Statements on websites

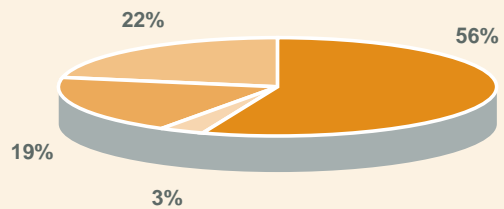
A WEBSITE PRIVACY STATEMENT IS NOT A PRIVACY POLICY

A Privacy Policy documents an organisation's application of the eight data protection principles to the manner in which it processes data organisation-wide. Such a policy applies to all personal data processed by the organisation, including customer data, third party data and employee data. The Privacy Policy can, in some instances, be a very complex document, having to apply the data protection principles to its own operating environment. The Privacy Policy is fundamentally a document for internal reference.

A Privacy Statement is a public declaration of how the organisation applies the data protection principles to data processed on its website. It is a more narrowly focused document and by its public nature should be both concise and clear. My website



Results of survey of Privacy Statements on Public Sector Websites



Total number of sites inspected	242
Number with no privacy statement	135 (56%)
Number with poorly placed privacy statement	8 (3%)
Number with poor content in privacy statement	46 (19%)
Number with adequate privacy statements	53 (22%)

contains guidance notes for preparing a privacy statement.

As Data Protection Commissioner I am concerned about privacy standards in the on-line environment. I have many times spoken in public about the need for those bodies collecting personal data on-line to have adequate privacy statements on their websites. A privacy statement is a means by which a data controller can demonstrably comply with the requirements of section 2D of the Data Protection Acts 1988 and 2003. Furthermore, Regulation 5 of Statutory Instrument 535 of 2003 [European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2003] also places obligations on persons controlling websites to, at least, provide information about the use of such technical features as cookies or the collection of IP addresses.

During 2004 my Office conducted a survey of Public Sector websites. Altogether, 242 sites were identified and contacted in respect of their use of Privacy Statements. Where organizations collected personal data on-line

and/or used technical features such as cookies my Office expected that the organisations concerned addressed this deficiency and that sites would contain an adequate privacy statement by no later than 31st January 2005. This matter is currently being reviewed. In all, the survey showed that 53 sites have adequate Privacy Statements; 46 have inadequate content in their Privacy Statements; 8 have poorly positioned Privacy Statements and 135 have no identifiable Privacy Statement. My staff are in the process of contacting those sites identified as having problems with their Privacy Statements. They shall also further assess those sites with no statements. After this final assessment, I may initiate enforcement proceedings against parties who are identified as non-compliant. A similar survey will be carried out during 2005 on private sector websites.

As indicated in Part 1 of this Report the Article 29 Working Party of EU Data Protection Commissioners during the year endorsed the principle that a fair processing notice on websites does not need to be contained in a single document but could be provided in up to three layers of information comprising a

- *Short notice*
- *Condensed notice and*
- *Full notice.*

Templates for the short and condensed Privacy Notices are available on the Article 29 website at http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp100_en.pdf. I commend them to data controllers as a model for informing data subjects about processing of their personal data. While these notices are more suitable for online activities they can easily be adapted for offline transactions provided an individual is given a simple means (e.g. a free phone number) to obtain detailed information.

My initial concern about the presence of Privacy Statements on websites was raised when I noted that many of the recipients of previous e-government awards had no Privacy Statements. It is disappointing to note that at the third annual Irish e-government awards in 2005 half of the recipients of awards had no Privacy Statements. This despite the fact that all those concerned actively collected personal data on their websites. I would expect that, by 2006, all the contenders will be compliant with their data protection obligations.

Appendix 8

Registrations 2002 / 2003 / 2004

	2002	2003	2004
(a) Public authorities and other bodies and persons referred to in the Third Schedule			
Civil service Departments/Offices	116	118	127
Local Authorities & VECs	139	138	144
Health Boards/Public Hospitals	57	59	60
Commercial State Sponsored Bodies	43	45	44
Non-Commercial & Regulatory	164	171	174
Third level	45	54	50
Sub-total	564	585	599
(b) Financial institutions, insurance & assurance organisations, persons whose business consists wholly or mainly in direct marketing, providing credit references or collecting debts.			
Associated Banks	42	46	46
Non-associated banks	58	62	66
Building societies	6	6	7
Insurance & related services	182	230	303
Credit Union & Friendly Societies	447	449	445
Credit Reference/Debt Collection	22	28	35
Direct Marketing	64	61	65
Sub-total	821	882	967
(c) Any other data controller who keeps sensitive personal data			
Primary & secondary schools	33	340	572
Miscellaneous commercial	79	77	130
Private hospitals/health	107	125	147
Doctors, dentists, health professionals	467	576	752
Pharmacists	667	828	850
Political parties & public representatives	95	108	156
Religious, voluntary & cultural organisations	91	118	152
Legal Profession	93	445	615
Sub-total	1,632	2,617	3374
(d) Data processors	412	524	549
(e) Those required under S.I. 2/2001			
Telecommunications/Internet Access providers	3	10	20
TOTAL	3,632	4,618	5509

Appendix 9

Office of the Data Protection Commissioner – Abstract* of Receipts and Payments in the year ended 31 December 2004

	2004 €	2003 €
Receipts		
Moneys provided by the Oireachtas	1,323,676	1,242,960
Registration Fees	530,854	455,539
	1,854,530	1,698,499
Payments		
Staff Costs	940,790	730,427
Establishment Costs	269,754	400,920
Education and Awareness	64,814	49,920
Legal and Professional Fees	21,683	48,107
Incidental and Miscellaneous	26,635	13,586
	1,323,676	1,242,960
Payments of Fees to the Vote for the Office of the Minister of Justice, Equality and Law Reform	530,854	455,539
	1,854,530	1,698,499

* 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.

Data Protection Commissioner

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

Tel. (01) 874 8544 Fax. (01) 874 5405
eMail. info@dataprotection.ie Web. www.dataprotection.ie

Coimisinéir Cosanta Sonraí

Bloc 6, An t-Áras Árachais, Sráid na Mainistreach Íochtarach, Baile Átha Cliath 1

Tel. (01) 874 8544 Fax. (01) 874 5405
Rphoist. info@dataprotection.ie Láithair Eangach. www.dataprotection.ie