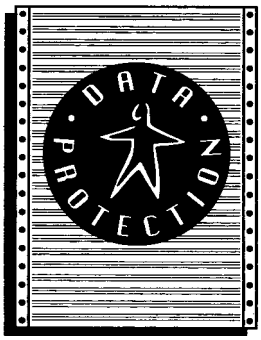


Eleventh Annual Report of the Data Protection Commissioner 1999

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

PN. 8848

FOREWORD

I hereby submit my seventh Annual Report to Dáil and Seanad Éireann pursuant to the provisions of section 14(1) of the Data Protection Act, 1988. This is the eleventh Annual Report submitted in relation to the work of the Office of the Data Protection Commissioner since it was established in 1989.

Fergus Glavey
Data Protection Commissioner
August, 2000

MISSION STATEMENT

To secure respect for the individual's right to privacy with regard to information held on computer about him or her by

- **upholding the rights and**
- **enforcing the obligations**

set out in the Data Protection Act, 1988

Office of the Data Protection Commissioner
Block 4, Irish Life Centre, Talbot Street, Dublin 1
Phone: (01) 874 8544 **Fax:** (01) 874 5405 **E-Mail:** *info@dataprivacy.ie*

CONTENTS

INTRODUCTION

THE IMPORTANCE OF DATA PROTECTION

Data protection law and practice are all about securing respect for the individual's right to private life. The right to private life has long been recognised in human rights charters such as the Universal Declaration of Human Rights of 1948 and the European Convention on Human Rights and Fundamental Freedoms, 1953. European data protection authorities are acutely conscious of the human rights origins of data protection, as can be seen from their comments in Appendix 5 on the recently mooted charter of fundamental rights in the European Union: *"Inclusion of data protection among the fundamental rights of Europe would make such protection a legal requirement throughout the Union and reflect its increasing importance in the information society."* The right to privacy is already acknowledged, either explicitly or implicitly, in the constitutions of many European democracies including our own Bunreacht na hÉireann. This right is to be valued for many inter-related reasons. Privacy, in the words of the Law Reform Commission[1], is *"closely connected to notions of inherent human dignity, ...to human freedom, autonomy and self-determination. ...It is an organising principle of civil society ...and is closely connected to the democratic life of the polity."* In the emerging information society, the values encompassed by privacy will be most disputed in relation to the control of information about people kept on computer.

Occasionally, commitment to securing respect for private life and privacy values in the information society is mistakenly portrayed as opposition to harnessing the benefits of advances in computing and communications technologies. Nothing could be further from the truth. However, a recurring theme in the annual reports of privacy and data protection commissioners worldwide is the need to ensure that man remains the master of the machine rather than become its servant or, perhaps more accurately, that the many do not become the servants of the few who control the use and application of information technology.

My experience suggests that there is a serious risk of minimising the capacity of the individual as decision maker, by de-personalising, and reducing the number of traditional information relationships, in favour of automated decision-making and direct exchanges of personal data between organisations . Over the years, I have found that some of the most intractable data protection issues arise from a belief by some organisations that they know what is best for their clients. This attitude is frequently accompanied by a marked reluctance to consult the same clients, be they customers or citizens, on decisions regarding the collection of information to be kept on computer about them, much less to offer them positive choices regarding the uses and disclosures of their personal data. To avoid such pitfalls, organisations should not presume to make key decisions regarding the use of their clients' personal data without consent, but should actively seek their guidance instead.

REVIEW OF DEVELOPMENTS IN 1999

This Annual Report gives a comprehensive overview of my Office's activities during 1999. The Report is divided into three Parts and seven Appendices.

[1] *Privacy, Surveillance and the Interception of Communications,* Law Reform Commission, June 1998

In **Part 1**, I review the day-to-day work of the Office. I describe the work done to promote awareness of data protection among data controllers and data subjects, with particular reference to the important task of influencing policy makers. I outline the enquiries and complaints handled in 1999, and comment on the future direction of registration in the light of the requirements of the European Union directive on data protection. I describe the growing importance of the international dimension of the work and conclude with some details of office administration.

Part 2 provides a selection of case studies which illustrates the application of data protection principles in real-life situations. They demonstrate the pervasiveness of information technology, and show how the thoughtless application of that technology can cause problems.

Part 3 of my Report, as in previous years, provides an in-depth analysis of some key data protection issues. This year, I have considered it timely to examine the question of data protection in the workplace, and to give a practical illustration of how the credit referencing system applies to individual borrowers.

Number 25 *of* 1988

DATA PROTECTION ACT, 1988

AN ACT TO GIVE EFFECT TO THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA DONE AT STRASBOURG ON THE 28TH DAY OF JANUARY, 1981, AND FOR THAT PURPOSE TO REGULATE IN ACCORDANCE WITH ITS PROVISIONS THE COLLECTION, PROCESSING, KEEPING, USE AND DISCLOSURE OF CERTAIN INFORMATION RELATING TO INDIVIDUALS THAT IS PROCESSED AUTOMATICALLY. [13*th July*, 1988]

BE IT ENACTED BY THE OIREACHTAS AS FOLLOWS:

Preliminary

Interpretation and application of Act.

1.—(1) In this Act, unless the context otherwise requires—

"appropriate authority" has the meaning assigned to it by the Civil Service Regulation Acts, 1956 and 1958;

"back up data" means data kept only for the purpose of replacing other data in the event of their being lost, destroyed or damaged;

"civil servant" has the meaning assigned to it by the Civil Service Regulation Acts, 1956 and 1958;

"the Commissioner" has the meaning assigned to it by *section 9* of this Act;

"company" has the meaning assigned to it by the Companies Act, 1963;

"the Convention" means the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data done at Strasbourg on the 28th day of January, 1981, the text of which is set out in the *First Schedule* to this Act;

"the Court" means the Circuit Court;

"data" means information in a form in which it can be processed;

"data controller" means a person who, either alone or with others, controls the contents and use of personal data;

INTRODUCTION

This opening Part of my Report fulfils the basic function of reporting upon the activities of my Office during the year 1999, and the progress that has been made across several fronts. I believe that this Part also serves to illustrate how diverse and wide-ranging the roles of my Office have become. From our most basic duties of informing the Irish public of their data protection rights and responsibilities, through to dealing with complex queries and complaints, to maintaining an extensive public register of data controllers, and to the ever-growing international commitments of my Office: all of these dimensions of the Office's work are reported upon in the following pages. The subsequent Parts will provide a deeper cross-section of aspects of the Office's work by focusing upon individual case studies and particular issues that may be of broader interest.

EDUCATION AND AWARENESS

The effectiveness of data protection law depends, in large part, on the extent to which individuals and organisations are aware of their rights and responsibilities under the Data Protection Act. I am also firmly of the view that when data controllers are fully apprised of their obligations, and when data subjects are equipped to exercise their rights, then the likelihood of inadvertent breaches of the Act is greatly diminished. For these reasons, I consider the promotion of awareness of data protection to be a key element of the work of my Office.

In pursuing this objective, my Office uses a number of avenues. In the first place, we produce a number of different leaflets and booklets which are aimed at providing useful information for data controllers and data subjects. My office issued approximately 23,000 such publications during 1999. The feedback that I have received suggests that these publications are found to be helpful to their target audiences. It is worth noting, however, that there are some constraints on the effectiveness of this approach in promoting overall awareness of data protection. Naturally, financial constraints preclude the Office from distributing the publications as widely as might be desired. The severe limitations upon the Office's staffing resources, to which I have consistently made reference over the years, inhibit the scope for proactive awareness initiatives. I am also mindful that the Data Protection Act, 1988 must be amended shortly, to transpose the European Directive 95/46/EC on data protection into Irish law. These major legislative changes will need to be coupled with a large-scale information and awareness campaign, and it would clearly be wasteful of scarce resources to initiate such a campaign in advance of the new legislation.

A second approach to promoting awareness of data protection is media advertising. My Office expended about £14,000 on advertisements and notices in 1999. The current advertising strategy is to ensure a mix between general reference material for the public (e.g. advertisements in telephone directories), and more sector-specific educational material for data controllers (e.g. advertisements in business publications and journals). This advertising has concentrated on general aspects of data protection law such as the "fair obtaining" principle and the access rights of data subjects, which are unlikely to be changed by forthcoming amendments to the 1988 Act.

Another way of increasing awareness about data protection issues among both "data subjects" — individuals about whom information is kept on computer — and "data controllers" — those who keep the information — is through direct contact between my Office and representative bodies and associations. It is my view that this approach can be very effective in disseminating practical knowledge and understanding among diverse groups of people, both data subjects and data controllers. An emphasis upon "training the trainers", i.e. educating those people who will be in a position to educate

others, is bound to multiply the effectiveness of the resources allocated to this area. It was for this reason, for example, that my Office provided input for the curriculum for the European Computer Driving Licence (ECDL), a programme to develop competence in the use of computer technology and an understanding of fundamental issues in information management. This programme is available for schoolteacher training in the Blackrock Education Centre, and deals with data protection issues in an accessible manner.

It is also my policy to respond positively, insofar as resources permit, to requests to deliver presentations on data protection matters to different groups. An insight into my Office's work in this regard may be had from the following presentations made by my Office over the past year.

Oireachtas Joint Committee on Enterprise and Small Business: E-commerce

A most important and very welcome request came from the Oireachtas Joint Committee on Enterprise and Small Business in the context of its consideration of e-commerce and related issues. I presented an overview of the 1988 Data Protection Act, highlighting its human rights origins and derivation from European law. I highlighted the importance of addressing information privacy and fair information practices, as, in my view, building citizen and consumer confidence is critical to the success of e-commerce and e-government initiatives. A number of internet privacy policy statements were considered for illustrative purposes, and I concluded with the principle that, at least insofar as data protection is concerned, what is illegal offline remains illegal online. Equally, what is legal offline, for example anonymous purchasing of goods and services for cash, should remain an option online. Since my presentation to the Oireachtas Joint Committee, EU Data Protection Commissioners, who meet in the Article 29 Working Party, have issued their preliminary views on e-commerce and data protection, and these are set out in Appendix 2 of this Report.

Royal College of Surgeons in Ireland / Institute of Public Administration

The RCSI and IPA run an annual Diploma Course in Management for Medical Doctors. This course includes a data protection module dealing with the obligations of medical doctors as regards handling of medical data, and the rights of patients to access their data. This module has been prepared by my Office, and has been presented annually by one of my staff.

Special Education Schools

A representative of my Office attended the 1999 annual general meeting of the National Association of Boards of Management in Special Education, held in Athlone, and gave a presentation on the application of data protection in an education context. One interesting subject dealt with was the implications of the future extension of data protection law to manual records, and the parallels between freedom of information law and data protection law in governing access by individuals to their own records.

Bank of Ireland Group Conference

I addressed the 1999 Bank of Ireland Group Conference in Cork, outlining my views on the requirements of data protection law as it affects the financial services sector, and dealing with matters such as credit referencing and internet banking.

Institute of Personnel and Development

The annual conference of the IPD, held in Dublin, brings together human resource managers from a wide range of private and public sector organisations. My Office has made a presentation to the annual conference for the last number of years, dealing with the implications of data protection law for the handling of employee data.

Dublin Institute of Technology / Institute of Direct Marketing

The DIT runs an annual Diploma Course in Direct Marketing, and my Office has presented the data protection module for the last number of years. The material presented in this context has examined, for example, the question of consent and "opt in" and "opt out" clauses where "personal data" — data relating to a living individual — is being obtained for direct marketing purposes, and possible changes in this area in the light of the EU Directive on data protection.

It is also noteworthy that a number of commercially-organised conferences dealing with data protection law were held during 1999, and my Office was pleased to contribute to the discussions. These conferences were well-attended, and this is indicative of a growing level of awareness and appreciation of the significance of data protection law among responsible data controllers in Ireland, and an appreciation that privacy and data protection are subjects of growing importance because of major change in both the technological and legal environments.

ENQUIRIES

A significant part of the work of my Office is made up of responding to requests for information and advice from the general public. As a public service office, I attach great importance to providing a high standard of customer service in dealing with such requests, whether they are from data subjects, data controllers, students, researchers or news media. Many of these requests are routine in nature, and my staff are in a position to provide instant responses. Recently, however, I have noticed an increased awareness of the more straightforward aspects of data protection on the part of data controllers and data subjects in the enquiries made to my office. The impression I form is that a growing number of people are familiar with the basic principles of data protection; and, as the principles are applied in practice, the number of new and complex issues which are encountered increases. I notice an increase in the level of queries relating to the possible impact of European Commission *Directive 95/46/EC*, which deals with data protection, upon Irish practices. My Office will continue to prioritise the provision of a high quality advisory service, on a free and confidential basis, with a view to addressing all such queries.

The number of external contacts dealt with by my Office rose from about 2,000 in 1998 to over 2,200 in 1999 — an increase of around 10%. About 1,700 of these contacts were telephone-based queries, an increase of about 200 over the 1998 figure. Of the remainder, most were on foot of written correspondence, and there was a comparatively small number of personal callers and contacts by way of e-mail.

It is noteworthy that of the 2,200 contacts, about 1,000 were from data controllers (broadly encompassing businesses, public sector bodies, representative associations, and solicitors or accountants acting on their behalf). The fact that so many data controllers consider it beneficial to seek guidance from my Office is very positive. It indicates a desire by data controllers to develop a privacy-friendly environment. About 800 contacts with my Office were from data subjects, with the remainder comprising students and researchers (over 350), the news media, and normal administrative contacts.

DATA SUBJECT QUERIES

As in previous years, the bulk of queries I received from data subjects in 1999 related to the standard data protection areas of credit referencing, direct marketing, and exercising the right of access. My staff are usually in a position to deal with such standard queries promptly, and I am pleased to report that the majority of individuals appear to be satisfied with the quality of service provided. Where general information on data protection is sought, my staff offer to post out an information pack explaining the

operation of the Act. Increasingly my staff are dealing with queries relating to the application of information technology in everyday life. Examples are the application of data protection rules to the internet, and electronic surveillance of employees. In Part 3 of this Report, I set out my prelimanary views on the issue of data protection in the workplace.

DATA CONTROLLER QUERIES

The number of queries from data controllers in 1999 (approximately 1,000) shows a 20% increase on the previous year. This is one area of increased workload that I welcome wholeheartedly. An increased interest in data protection by data controllers results in an improved privacy environment for data subjects. My experience is that data protection infringements on the part of a data controller usually arise from ignorance of the law, inadvertence or negligence, as distinct from any deliberate disregard for privacy rights. While this distinction should not be taken as excusing ignorance or negligence on the part of a data controller, it does mean that when these deficiencies are addressed, then data subjects are bound to benefit. Accordingly, my staff make every effort to assist data controllers who contact my Office when planning their information systems.

COMPLAINTS

When a complaint is received, it is my Office's general practice to attempt to mediate between the parties involved, with a view to reaching a satisfactory resolution of the matter. As in previous years, my Office managed to resolve the greater proportion of complaints on an informal basis, without a requirement for me to instigate a full investigation leading to a formal decision as provided for in section 10 of the Act. Part 2 of the Report sets out a number of detailed case studies which give a flavour of the type of complaints dealt with in the past year.

1n 1999, I received one hundred and five complaints from individuals who felt that their rights under the Data Protection Act had been infringed — an increase of 35% on the previous year. One possible explanation for this increase is that, as people become increasingly familiar with the advantages and disadvantages of the information society, they are — quite rightly — exercising their rights and insisting on their entitlements with a greater degree of confidence than heretofore. Equally, the increasing technological sophistication of business life, in particular the growth of e-commerce, means that data controllers are having to deal with a wider range of data protection issues. I envisage that my Office will be called upon to play an increasing role in ensuring that individuals' rights are upheld in the era of e-commerce and e-government.

REGISTRATION OF DATA CONTROLLERS AND DATA PROCESSORS

Registration is a process whereby data controllers and data processors put on public record a summary of their policies and practices in regard to personal data. Ireland has a system of selective registration. Certain categories of data controller — such as financial institutions, direct marketing businesses and the State sector — must register annually with my Office, detailing *inter alia* the types of personal data collected by the data controller, the purposes for which the data are kept, and the persons to whom the data may be disclosed. This register is available in my Office for public inspection, free of charge. The registration process also serves the valuable function of establishing channels of communication between data controllers and my Office, and alerting them to their obligations under data protection law.

Appendix 6 gives a detailed sectoral breakdown of registered data controllers. The increase in the number of registered data controllers and data processors over recent years is shown in the table below.

year	1994	1995	1996	1997	1998	1999
no. of registrations	1,994	2,082	2,353	2,571	2,650	2,775
annual increase	7%	7%	13%	9%	3%	5%

It is interesting to note that the existing registration system in Ireland may have to be modified to ensure full compliance with the provisions of the EU Directive 95/46/EC on data protection. Under our existing system, data controllers do not need to register unless they are data controllers referenced in ***section 16*** of the *Data Protection Act, 1988.* The EU Directive, on the other hand, provides in Article 18 for a system whereby all data controllers must "notify" the data protection authority before carrying out automatic processing of data. Member States may provide for simplification or exemption from notification in cases where the data processing operations are *"unlikely to affect adversely the rights and freedoms of data subjects"*.

Data controllers await with interest proposals from the Minister for Justice, Equality and Law Reform to amend the 1988 Data Protection Act to give effect to the provisions of the Directive. Proposals to modify the existing registration system to take account of the new notification requirements will, in my view, be of particular interest. From the point of view of continuity for data controllers, the objective should be to minimise any disruption or confusion caused by the changeover to a new notification system. Changes in those who are currently required to register should be kept to a minimum. Certainly, a move to a universal notification system for all data controllers — including, for example, small businesses who do no more than keep payroll data in respect of their employees — would, in my opinion, be unlikely to contribute significantly to securing data subjects' privacy rights, and would moreover be wholly impracticable from the point of view of the administration system in my Office, unless significant extra staffing and other resources were made available.

Finally, I note that the existing registration system makes it reasonably clear-cut whether or not a particular data controller needs to register with my Office. Certainty and clarity of this nature are desirable principles of public administration, and should be preserved in the new arrangements. It would be a pity indeed if the existing registration system, which meets its objectives in a streamlined and cost-effective manner, were to be replaced with a notification system that was unduly burdensome both for data controllers and for this Office.

INTERNATIONAL

It is a truism to say that the revolution in information and telecommunications technology has shrunk the world. Every day many more of our citizens use the internet to access information, exchange correspondence and purchase goods and services. These technologies recognise no national boundaries, and, if data protection law claims to provide an ethical and legal framework for fair information practices in this new environment, it can be no surprise that it has a strong international flavour. This is manifest in the day-to-day operations of all data protection authorities. It is also fair to say that a small office such as this could not, in isolation, come up with effective solutions to the variety of privacy issues presented by the global information society. My Office benefits greatly from its international contacts in the development of its ideas. This section outlines some of the major international activities of my Office in 1999.

Article 29 Working Party

Directive 95/46 EC on data protection establishes two groups which are of significance for (a) the development of data protection within the EU, and (b) safeguarding the data protection interests of EU citizens when their data is transferred outside the EU. The first of these groups is the Article 31 Committee, comprising representatives of the Member States and chaired by a representative of the EU Commission. Its task is to assist the Commission particularly in relation to the important matter of decisions on the "adequacy" or otherwise of data protection regimes in countries outside the EU. The second group, which more directly influences the day-to-day workings of data protection authorities in the Member States, is the Article 29 Working Party. This group is composed of representatives of the Member States' independent data protection authorities, along with a representative of the EU Commission. The Working Party's role is advisory and it acts independently. In 1999, during which time it was chaired by the Dutch Data Protection Commissioner, the Working Party was particularly busy, not least because of the work involved in connection with the prolonged and difficult discussions between the USA and the EU on the important topic of transfers of personal data from the EU to the USA and the role of "safe harbours" in such transfers. I am glad to note that these discussions were satisfactorily finalised in the middle of the year 2000, and full details of this matter, including a copy of the "safe harbour" principles and accompanying documentation, can be found at the European Commission's web-site at the address:

http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

The Working Party also produced opinions on the "adequacy" of the data protection regimes in third countries such as Switzerland and Hungary. These opinions influence the Article 31 Group and the Commission in taking decisions on whether the data protection regime in the third country is adequate for the purpose of transferring personal data from the EU. The importance of such a finding is twofold. Firstly, it provides an assurance to EU citizens that their information privacy and data protection interests are likely to be respected on the transfer of their data to a data controller in the third country in question; and that if difficulties should arise, appropriate means of redress are available. Secondly, it facilitates the lawful transfer of personal data by Irish and other EU-based data controllers to the countries in question. This is of great importance from the viewpoint of encouraging e-commerce and the development of the global information society.

In 1999 the Article 29 Working Party also considered such important issues as: model contract clauses proposed by the International Chamber of Commerce for the export of personal data; a code of practice for direct marketing proposed by the Federation of European Direct Marketing Agencies; concerns deriving from the identification capabilities of the Intel Pentium III chip; the preservation of traffic data by Internet Service Providers; and problems associated with reverse telephone directories. On this last point, on which the Working Party's opinion will be published shortly, my Office was in a position to make a significant contribution to the formulation of policy, in light of our experience on this matter (see Case Study 8 on page 25 of this Report). A selection of the most significant publications of the Working Party is listed in Appendix 1, and a number of these documents, which may be of particular interest to Irish data controllers, are reproduced in full in Appendices 2-5.

Europol and Related Third Pillar Matters

As indicated in my previous Reports, there are two important dimensions to data protection work associated with the "European Police Office", or "Europol" as it is commonly known. Both dimensions derive from the Europol Act, 1997. The first of these is my Office's role as the National Supervisory Body responsible for ensuring that the data protection rules are complied with in the transfer of personal data from Ireland to Europol. The second aspect concerns the supervision of Europol itself from a data

protection point of view. This latter task took precedence over domestic supervision of data transfers to Europol in 1999, owing to (a) a lack of staff resources, and (b) my commitments as chairman of the Europol Joint Supervisory Body (JSB).

Considerable progress has been made in putting the work of the JSB on a sound footing, through the establishment of sub-groups dealing with particular matters, such as orders opening a data file under Article 12 of the Europol Convention, and the data protection inspection and audit of Europol's activities. The objective of the JSB has been to facilitate the work of Europol through the provision of timely opinions on data protection matters, while ensuring that sound practice in this regard becomes the norm in Europol, thus safeguarding the data protection rights and freedoms of individuals whose personal data is kept by Europol. The work of the JSB was greatly facilitated in 1999 by the establishment of the practice of back-to-back meetings in Brussels with the Schengen Joint Supervisory Authority. I am particularly grateful for the co-operation of my JSB colleagues in making this progress possible, and for the assistance of the secretariat now provided by the Council. I wish to express my particular thanks to Mr Niels Bracke for all his help and hard work.

It seems to me that the working methods of the Europol JSB are now well established, and that the road ahead for further co-operation between the data protection supervisory bodies of Europol, Schengen and the Customs Information System, and perhaps other similar entities, is well sign-posted. The culmination of the work done in this area, particularly in 1999, is to be found in the draft Council decision establishing a common secretariat for the data protection supervisory bodies mentioned above. The work on this project, which was initiated at the 1998 Spring Conference in Dublin, was finalised by the Council's Portuguese Presidency, and is currently being examined by the European Parliament. I expect that the new and very welcome arrangements will come into effect in 2001. Notwithstanding this progress on institutional and procedural questions, much remains to be done, given the diversity in the substantive data protection rules to be found in the various third pillar instruments. This work will involve not only an analysis of the rules themselves, but also an assessment of whether the differences are a reflection of policy choices or are merely the result of historical accidents.

Meetings of Data Protection Commissioners

The Article 29 Working Party, the Europol JSB and similar bodies are noteworthy for the organisational support provided by virtue of their derivation from specific legal instruments such as Directive 95/46 EC, and the provision under such instruments of a budget and a secretariat. However, other important meetings are organised by the community of data protection authorities on a voluntary basis. The most important of these are the Spring Conference of European Data Protection Commissioners and the International Conference on Privacy and Personal Data Protection. The Spring Conference was held in Helsinki, Finland, in 1999, and considered topics including "The Future of Privacy Audits in Europe", "Ethical Issues in Genetic Testing" and "Schengen and Data Protection Questions". The 1999 International Conference was held in Hong Kong. This Conference addressed questions concerning "The Emerging Law of Cyberspace and Implications for Data Protection", "Consumer Rights in Electronic Commerce", "Privacy and the News Media" and "Data Protection and Freedom of Information: Two Sides of the Same Coin", at which I made a presentation drawing upon the Irish experience.

Meetings between my Office and my counterparts in the United Kingdom, Guernsey, Jersey and the Isle of Man are held annually. The 1999 meeting was held in Manchester, and the opportunity was taken to explore developments of common interest in the areas of credit referencing and data matching. As in previous years, my staff and I found these meetings to be particularly productive, as the experience gained in the British jurisdictions is often readily applicable in the Irish context.

ADMINISTRATION

PAYMENTS AND RECEIPTS

The cost of running the Office in 1999 was £392,525, an increase of 7.8% on the previous year. An analysis of these costs is given in Appendix 7 (pages 57-59). Receipts from registration fees amounted to £233,674, offsetting 60% of the cost of running the Office. Income from registration fees increased by 5.8% on 1998.

STAFF

I have a team of seven staff. Since my last Annual Report Ms Anne-Marie Lynch has moved to other duties on promotion and Ms Avril Brady has taken a career break. I wish to thank both for their contribution to the success of the office in the past, and to wish them well in their future careers. I am glad to welcome their replacements, Ms Breda Purcell and Ms Pamela Smith, and to thank them and the other members of the team, my Deputy Mr Tom Lynch, Mr Ronnie Downes, Ms Anne Gardner, Mr Sean Sweeney and Ms Irene O'Keeffe for their continuing support. The numbers and complexity of the enquiries they have dealt with in 1999 is a tribute to their professionalism and commitment to delivering a quality service to the public, be they data subjects or data controllers.

While I am fortunate to have the commitment of this team, this does not obviate the fact that my Office is seriously understaffed. In my Report for 1998 I noted that this had been the position for several years past, and that additional staff were essential if any reasonable level of service to the public was to be maintained. This remains the position, and in my view there is no possibility of the Office coping adequately with the increased workload which will flow from the new legislation necessary to transpose Directive 95/46/EC into Irish law without a significant increase in staff. I well appreciate that when the Office was established more than ten years ago the economic and budgetary climate was unfavourable. However it is hard to argue that this is still the case, and in my view it is essential to put the Office's staffing on a proper footing sooner rather than later. Failure to do so would be quite inconsistent, in my view, with the crucial role of data protection in securing fair information practices for individual citizens in the information society.

SUPPORT SERVICES

The administration of the Office in 1999 faced additional pressures owing to the need to prepare and implement a Year 2000 computer strategy. I am glad to record that such a strategy involving the replacement and upgrading of much of the Office's computer hardware and software was successfully concluded with the help and cooperation of the Department of Justice Information Technology Unit. The necessity to make these changes was used as an opportunity to review and modify many of our office procedures. Regrettably, the pressure of making these changes on the very limited staffing resources available made it impossible to develop an Office website in 1999. This is a disappointment given the contribution such a site could make to all aspects of the work of the Office, and especially to the drive to improve data protection education and awareness.

As always, the Finance Division of the Department of Justice, Equality and Law Reform continued to provide my Office with an excellent service in relation to receipts and payments in 1999, and I should like to express my appreciation of their helpfulness.

Number 25 *of* 1988

DATA PROTECTION ACT, 1988

AN ACT TO GIVE EFFECT TO THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA DONE AT STRASBOURG ON THE 28TH DAY OF JANUARY, 1981, AND FOR THAT PURPOSE TO REGULATE IN ACCORDANCE WITH ITS PROVISIONS THE COLLECTION, PROCESSING, KEEPING, USE AND DISCLOSURE OF CERTAIN INFORMATION RELATING TO INDIVIDUALS THAT IS PROCESSED AUTOMATICALLY. [13*th July*, 1988]

BE IT ENACTED BY THE OIREACHTAS AS FOLLOWS:

Preliminary

Interpretation and application of Act.

1.—(1) In this Act, unless the context otherwise requires—

"appropriate authority" has the meaning assigned to it by the Civil Service Regulation Acts, 1956 and 1958;

"back-up data" means data kept only for the purpose of replacing other data in the event of their being lost, destroyed or damaged;

"civil servant" has the meaning assigned to it by the Civil Service Regulation Acts, 1956 and 1958;

"the Commissioner" has the meaning assigned to it by *section 9* of this Act;

"company" has the meaning assigned to it by the Companies Act, 1963;

"the Convention" means the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data done at Strasbourg on the 28th day of January, 1981, the text of which is set out in the *First Schedule* to this Act;

"the Court" means the Circuit Court;

"data" means information in a form in which it can be processed;

"data controller" means a person who, either alone or with others, controls the contents and use of personal data;

INTRODUCTION

In the Annual Reports produced by my Office over the years, it has become traditional to include examples of "real world" cases with which I have dealt, in order to illustrate the practical application of the principles set out in the legislation. In the absence of any significant body of case law dealing with data protection in Ireland, the case studies hopefully serve a useful function in giving guidance to both data controllers and data subjects. The great majority of the complaints and queries dealt with by my Office tend to be quite similar in nature from one year to another, and it is important that businesses, the public services and the general public have the opportunity to learn from the experience of others. At the same time, data processing by its nature is a rapidly evolving field, and new questions and unexpected issues arise continually. It is important that data controllers have some degree of certainty as to how these issues are likely to be addressed, in order that businesses — particularly those operating in technically innovative areas — can take decisions on a sound and legally sustainable basis. Case studies can play a role in this regard, by providing data controllers with an insight into issues that may be of concern for them. In the cases that follow, I therefore deal with a wide variety of data protection issues. Some of these issues might be characterised as the traditional staple diet of a data protection authority, including complaints about direct marketing questionnaires *(Case Study 1)* and inaccurate credit ratings *(Case Study 6)*. Other examples deal with technical and legal points that may be of interest to data controllers generally — for example the requirement to keep personal data secure *(Case Study 2)*, the question of whether word-processed documents on computer constitute "data" for the purposes of the Act *(Case Study 4)*, and an issue of whether the disclosure of names is sufficient to constitute a "disclosure" of data *(Case Study 9)*. *Case Study 8* deals with the conversion of a manual directory of personal data into electronic form. *Case Study 10* is of significance because the case is one of the very few to have given rise to an Appeal to the Circuit Court from a Decision of the Data Protection Commissioner.

CASE STUDY 1 — mass circulation questionnaire - apparent official nature of the questionnaire - compilation of lifestyle databases - whether data fairly obtained - assistance of United Kingdom data protection authority

I received several complaints from persons who had received a "lifestyle" questionnaire through the post. The questionnaire, which appeared to be for purposes of "national research", sought very detailed information regarding the recipient's hobbies, shopping habits and household finances. The complainants were concerned that the questionnaire, which was a commercial information-gathering exercise, sought to mimic the style of official Government surveys and was at the very least a breach of the spirit of data protection legislation. Concerns were also expressed that the provision for an opt-out from direct marketing was wholly inadequate by virtue of its size and location.

In investigating this complaint, I established that the questionnaire was (a) devised by a United Kingdom direct marketing and market research company which specialised in the compilation of "lifestyle databases", and (b) issued by an Irish company who returned the completed survey forms direct to the UK without "processing" (within the meaning of the Data Protection Act) the information in any way. Such databases, which in the UK contain several millions of records, are built from responses to mass circulation questionnaires. I consulted my United Kingdom counterpart, who advised me that her Office regularly monitors the compilation and use of such large marketing databases. She indicated that discussions are ongoing between her Office and the companies involved, with a view to securing changes in survey forms of this kind so as to make more transparent who is collecting the data, the purposes for which the data will be used and to whom they will be disclosed.

In assessing what action to take in dealing with these complaints, I had regard to ***section 2(1)(a)*** of the *Data Protection Act, 1988* which provides as follows —

A data controller shall, as respects personal data kept by him, comply with the following provisions:
(a) the data or, as the case may be, the information constituting the data shall have been obtained, and the data shall be processed, fairly ....

I have consistently expressed the view to data controllers that I consider fair obtaining to be an active duty, and that it is up to a data controller keeping personal data to make sure that such data have been fairly obtained. A booklet titled *"Keeping Personal Information on Computer: Your Responsibilities"* is distributed widely to data controllers by my Office. In it, I explain that for a data controller to satisfy the requirements of fair obtaining and purpose specification, he or she must ensure that —

(a) At the time of providing personal information, individuals are made fully aware of:

- *the identity of the persons who are collecting it (though this may often be implied)*
- *to what use it will be put,*
- *the persons or category of persons to whom it will be disclosed.*

(b) Secondary or future uses which might not be obvious to individuals should be brought to their attention at the time of obtaining personal data. Individuals should be given the option of saying whether or not they wish their information to be used in these other ways ... .

These are the ways a data controller achieves ***transparency*** *and* ***informed consent*** *— the touchstones of fairness in data protection.*

On examining the questionnaire and the accompanying documentation, I noted that the covering letter identified the promoter of the survey, whose address was given in full. The documentation also stated that the information supplied would be made available to other companies for the purpose of direct marketing, and that individuals could decline to receive additional offers by ticking a box. The complainants' difficulties (with which I sympathised) derived not so much from what was said in the documentation but from the way in which it was presented. On balance, I decided that the appropriate course of action was to —

- write to the Irish distributor of the questionnaire urging him not to circulate any further surveys of this nature without prior discussion with my Office;
- write to the UK data controller about the complainants' concerns regarding (a) the misleading nature of the questionnaire and (b) the inadequacy of the "opt out" clause; and
- pursue further progress on this general matter in consultation with my UK colleague.

This case well illustrates the very real impact a data controller operating from outside the State may have on Irish data subjects and the issues this gives rise to for both the harmonisation of data protection laws and the common interpretation of data protection principles such as "fair obtaining". It also illustrates the issues which arise both for the investigation of complaints and follow-up action where the data subject is in one jurisdiction and the data controller in another. Many of these questions are as yet unresolved though it can be expected that solutions will be found through the workings of the *Article 29 Working Party* referred to elsewhere in this Report. In the meantime, my advice to data subjects is to simply ignore lifestyle questionnaires of the kind described if they have the slightest doubt as to their provenance or the purposes for which they are really issued.

CASE STUDY 2 — life insurance company - retention by ex-employee of customer data - unauthorised access - obligation to take appropriate security measures

The complainant was a long-standing customer of a particular life insurance company. One of the company's representatives, who had in the past been dealing with the customer's affairs, left the company to join a different company in the same line of business. He subsequently called to the complainant and asked her if she would like to transfer her policies to the company he now represented, or take out new policies with this company. The complainant said that she did not have documents relating to her existing policies to hand. At this, the representative opened his laptop computer and accessed details of her existing policy, notwithstanding the fact that he now represented an entirely different insurance company.

The customer was very unhappy that confidential personal data relating to her insurance were still available to an ex-employee of her insurer who now worked for a competitor. She took the matter up with her insurer but was not satisfied that the breach of confidentiality was treated with the seriousness it deserved. She then wrote to me to complain about the matter.

Section 2(1)(d) of the *Data Protection Act, 1988,* provides that —

> *Appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of [personal data] and against their accidental loss or destruction.*

I wrote to the complainant's insurer and asked them to comment on the case in the light of this provision. I also asked the company to provide further details on the background to the case and to outline its security arrangements.

The company responded by explaining that the nature of its business (with a direct sales force operating at locations nation-wide) required that the company's field representatives should have access to client information on laptop computers. Representatives were under clear instructions that, if they left the company's employment, they should return all company records and documents to their immediate supervisor. Supervisors were under instruction to ensure that this happened. The company said that in the case of the former employee involved in this case, these procedures had not been complied with. Numerous attempts had been made to recover the laptop and the client data from the former employee. However he did not return phone calls or meet with company officials. Attempts to recover the client data were ongoing, according to the company, at the time of the events giving rise to the complaint.

With regard to the requirement to keep personal data secure, the company said that it had put new procedures in place, so that client data would automatically be erased from laptop computers every six weeks, unless a representative's authorisation was renewed. When these matters were explained by my Office to the complainant, she was reassured that the company was now taking its data protection obligations as regards security seriously and that, accordingly, breaches of confidentiality of the kind she had encountered were unlikely to recur.

In my view, this case illustrates the need for data controllers to have firm and enforceable procedures in place to ensure that they do not lose control of personal data, for which they are legally responsible, on the departure of any of their employees. Provision for the automatic deletion of records, of the kind now put in place by the company, may have a useful part to play in such arrangements.

CASE STUDY 3 — Vehicle Registration Unit - disclosure of names and addresses to a motor distributor - disclosure required by law

The complainant owned a particular make of car. He received a letter from the motor distributor advising him of a technical fault and offering to repair the fault for him. The letter indicated that the

distributor was able to contact him directly through the co-operation of the Vehicle Registration Unit (VRU) of the Department of the Environment and Local Government. The complainant raised the matter with me, and expressed his concern that the VRU should pass his personal details to third parties. He had thought that only the Gardaí and certain Government Departments could access car registration data.

I raised the matter with the Department of the Environment and Local Government, and asked for their observations on the matter in the light of ***section 2(1)(c)(i)-(ii)*** of the Data Protection Act, which provides that personal data *"shall be kept only for one or more specified and lawful purposes"*, and *"shall not be used or disclosed in any manner incompatible with that purpose or those purposes"*.

In its response, the Department cited ***section 60(3)*** of the *Finance Act, 1993,* which provides as follows—

> *An officer of a Minister of the Government, a licensing authority or the competent authority for licensing vehicles and drivers of vehicles in another Member State of the European Communities, an officer of the Revenue Commissioners, a member of the Garda Síochána or such (if any) other persons as may be prescribed shall have access to and may inspect and examine records established under this section.*

The *Finance Act, 1993 (section 60) Regulations, 1996* (S.I. Number 338 of 1996) include *"motor vehicle manufacturers and distributors"* among the persons prescribed for the purposes of section 60.

Section 8(e) of the Data Protection Act provides that —

> *Any restrictions in this Act on the disclosure of personal data do not apply if the disclosure is... required by or under any enactment or by a rule of law or order of a court ...*

In my opinion, section 60, taken together with the regulations cited above, gives motor vehicle manufacturers and distributors access to vehicle registration and driver licensing records. It appears to me that a disclosure of personal data in compliance with section 60 comes within the scope of section 8(e) of the Data Protection Act, and therefore any such disclosure is not restricted by the Data Protection Act.

The Department of the Environment and Local Government pointed out to me that it is always conscious of maintaining the confidentiality of individual vehicle owners as recorded on the National Vehicle and Driver File (NVDF). Apart from specified Government Departments and Offices who require access to the vehicle records to carry out their functions, the Department assured me that the disclosure of details from the NVDF to any other third parties was strictly precluded. The Department indicated that a single exception to this principle is applied where the Department is satisfied that, in the interests of the safety of vehicle owners and other road users, data from the computer file should be provided to assist motor companies with recall campaigns where defects had been detected in particular models. I welcome this statement of policy which seems to me to strike a reasonable balance between protecting the privacy interests of data subjects whose data is kept on the NVDF, and the public interest in ensuring that defective vehicles are recalled as swiftly as possible. It was such a consideration that led the VRU to disclose details to the motor distributor in this case.

However, I have a residual concern that the inclusion of "motor vehicle manufacturers and distributors" in the regulations, coupled with the unqualified words *"shall have access to"* in section 60 referenced above, may have more far reaching consequences than are at first apparent and I suggest that this be reviewed when a suitable opportunity arises.

CASE STUDY 4 — State agency - subject access request - whether word-processed documents retained on computer constitute "data"

The complainant had dealings with a State agency. He made an access request under ***section 4*** of the Data Protection Act to be provided with a copy of all data held by the agency relating to him. The agency responded by providing him with some records. The complainant was engaged in legal action against the agency, and in that context he had obtained an order of discovery against the agency. Arising from this order, the complainant had reason to believe that some data relating to him had not been supplied to him by the agency, and he complained to my Office.

I took the matter up with the State agency, which was happy to co-operate with my enquiries. I drew the agency's attention to the apparent existence of some records held on computer relating to the complainant, which had not been included in the agency's response to the access request. The agency expressed surprise at this apparent discrepancy, and undertook to re-examine their response to the complainant's original access request.

Having looked into the matter, the agency established that a significant number of word-processed records, the contents of which related to the complainant, were kept in different units throughout the organisation, and that some of these records were kept on computer. Because these records were not readily accessible by the central administrative office that had handled the original access request, they had not been considered for release in response to the complainant's access request. Moreover, the agency questioned whether these word-processed records constituted "data" for the purposes of the Act, and whether there was any requirement to include these records in responding to the access request. In support of their case the agency cited the definitions set out in ***section 1(1)*** of the Act as follows —

> *"data" means information in a form in which it can be processed*
>
> *"processing" means performing automatically logical or arithmetical operations on data and includes —*
>
> *(a) extracting any information constituting the data, and*
>
> *(b) in relation to a data processor, the use by a data controller of data equipment in the possession of the data processor and any other services provided by him for a data controller,*
>
> *but does not include an operation performed solely for the purpose of preparing the text of documents.*

The State agency suggested that the definition of *"processing"*, from which the operation of text-preparation is specifically excluded, put computer records of word-processed documents outside the scope of the Act, since such records did not constitute information in a form in which it could be "processed".

I did not accept the agency's argument on this point. In the first place, I explained that the definition of *"processing"* specifically includes the process of *"extracting any information constituting the data"*. As the information in question had been retrieved from the word-processed records, this process of extraction had obviously been performed. Second, I noted that *"preparing the text of documents"* is a finite process, which concludes once, say, a letter has issued, or the note of a meeting has been finalised, as the case may be. If subsequently any processing operation can be performed upon the word-processed record, such an operation cannot be *"solely for the purpose of preparing the text of documents"*, whatever else the purpose may be. Accordingly, I was of the opinion that word-processed records, which were kept on computer or on computer media after the document in question had been finalised, constituted "data" for the purposes of the Data Protection Act and therefore must be

considered when responding to an access request from a data subject. The State agency in question agreed to provide the word-processed records to the complainant.

In my view, this case illustrates the significant implications that may arise for a data controller in the absence of a clear policy regarding the retention and deletion of computer records, including word-processed documents, from computer systems. Data controllers who do not delete word-processed documents from a computer once "preparation" is completed should be aware that they are keeping computer data which may well be accessible by a data subject. Indeed, *Directive 95/46/EC* makes no exemption for "text preparation", nor distinguishes in principle between manual files kept in a "structured" (or organised) filing system and computer records; and accordingly such exemptions and distinctions will become irrelevant, for data protection purposes, over time.

CASE STUDY 5 — voluntary organisation - role in administration of an official scheme - collection and use of RSI numbers - failure to register as a data controller

A small number of voluntary organisations were authorised by a State body to assist in the administration of an official scheme. The scheme was designed to benefit a certain category of individuals, many of whom would be represented by the voluntary organisations. Applications for participation in the scheme were made through the voluntary organisations, and in this context applicants were asked to supply their Revenue and Social Insurance (RSI) number.

I received a complaint from an individual who objected to the collection of RSI numbers by one of the voluntary organisations in question. The complainant was unhappy that the voluntary organisation, which was not an official State body, had access to the RSI number, which was also used in connection with his health and social welfare entitlements, and in connection with his tax affairs. Allowing a private body to hold his RSI number would, he feared, put at risk the privacy of his dealings with the State sector. The complainant also noted that the voluntary organisation in question was not registered with my Office, as was required under the Act.

I approached the organisation and asked why it was seeking RSI numbers from applicants. The organisation explained that the number was used to avoid duplications that might arise among the different organisations which were administering the scheme. Most adults had a unique RSI number, and so it was a handy identifier for applicants. I pointed out to the organisation my view that widespread and unregulated use of the RSI number, beyond the limited purposes for which the number had been instituted, could, over time, lead to an erosion of citizens' privacy. Having considered my viewpoint, the voluntary organisation agreed to stop using the RSI number, and to look for other ways of meeting its administrative needs. The organisation also accepted that it had failed to register with my Office, as required by ***section 19*** of the Data Protection Act, and it took steps to regularise the position.

The issue was solved to the complainant's satisfaction through the co-operation of the data controller. However, this case study raises interesting questions regarding the use of what is now the Personal Public Service Number (PPSN), in the light of the provisions of Part IV of the *Social Welfare Act, 1998*. This Act regulates the use of the PPSN and specifically limits its use to specified bodies. It appears to me that it is for the Department of Social, Community and Family Affairs, in the first instance, to ensure compliance with the requirements of Part IV of the Social Welfare Act, 1998. However, a data controller who, in contravention of the Social Welfare Act, 1998, *"uses a personal public service number or seeks to have a personal public service number disclosed to him"* may also face difficulties under the Data Protection Act, 1988. It is difficult to see how such a data controller could demonstrate that personal data had been "fairly obtained" as required by ***section 2(1)(a)*** of the Data Protection Act, where his or her acquisition of the PPSN contravened the Social Welfare Act, 1998. In my view, unlawfully obtained

personal data could not meet the "fair obtaining" criterion of the Data Protection Act. In this connection, it is worth recalling that when the then *Data Protection Bill, 1987* was being debated, the then Minister for Justice, in response to a proposed amendment, commented as follows: *"I have been advised that the obligation already imposed by the subsection to obtain fairly data or information constituting data would amply comprehend also obtaining it lawfully and with due regard to the data subject's constitutional rights."*

CASE STUDY 6 — financial institution - inaccurate credit rating - rectification - notification of third parties to whom incorrect data had been released

The complainants in this case were refused a loan from two financial institutions. They made an access request under the Data Protection Act to a credit bureau to see their credit records. The records indicated that they had in the past taken out three loans with a third financial institution ("Institution A"). While the two most recent loans were shown as having been paid off, the first loan (which had been taken out about six years previously) still appeared to be outstanding as it did not have a reference code to show that it had been paid. In fact, all three loans had been repaid on time.

The complainants took the matter up with Institution A, which had lodged the details with the credit bureau. On reviewing the details, the institution confirmed that the code, showing the first loan to have been completed, had been omitted from the record, and the institution said it had now returned the correct information to the credit bureau. Institution A also said that, notwithstanding the error, the individuals' credit record showed a satisfactory credit approval rating.

The individuals complained to my Office about the inaccuracy of their credit record. I asked Institution A for its views on the matter, in light of the requirement at ***section 2(1)(b)*** of the Data Protection Act that the personal data kept by a data controller *"shall be accurate and, where necessary, kept up to date"*. Institution A said that, "due to an administrative error", a return had not been sent by the institution to the credit bureau when the loan had been settled. The institution also claimed that the omission would not have prejudiced the complainants in any way: any other financial institution considering the credit record would know that the first loan must have been paid, because Institution A would not otherwise have given a second and third loan to the same individuals. Finally, the institution said that the human error involved in the case could not be repeated, as the manual method of making returns to the credit bureau had since been replaced with an automated system.

Arising from my Office's investigation of the case, I issued a formal decision in which I concluded that Institution A had failed to keep personal data in respect of the complainants up to date, as required by the Act, and accordingly I upheld the complaint. I rejected the argument that other financial institutions could have inferred that the original loan must have been repaid, as I noted that the second and third loans had been issued before the term of the first loan had expired. While taking account of Institution A's prompt action to correct the inaccurate record as soon as the error was brought to its attention, I explained that the Data Protection Act places a clear and active obligation on data controllers to ensure that data is kept accurate and up to date. In the circumstances, I recommended that the institution should contact all parties who had accessed the inaccurate credit record, notifying them of the correct position. Institution A subsequently complied with this recommendation.

I would emphasise to all data controllers their obligation to ensure the accuracy of their computer records. This is especially important where, as in the case of credit records, inaccuracies can have a significant bearing on people's livelihood. In this regard, data controllers should be aware of ***section 7*** of the Data Protection Act, which provides that individuals may take a civil action against a data

controller, where the individual has suffered damage as a result of the data controller's failure to comply with the requirements of the Act.

CASE STUDY 7 — debt collection service - acting on behalf of hospital - whether data had been "disclosed" for purposes of Data Protection Act - whether debt-collecting agency is entitled to build database of debtors

The two complaints in this case study arose from the actions of a hospital and a debt collection company. The first complainant, an elderly man, attended the hospital on a number of occasions for medical treatment. The hospital subsequently sent him a bill for the treatment. He paid some of the outstanding amount, but he did not pay the full amount straight away. After a period, he was contacted at home on his unlisted telephone number by a debt collection service. The debt collection service said it was acting to recover the hospital's money. The second complaint was from a young college student who had attended the same hospital and had been written to by the same debt collection service in similar circumstances. The agency wrote to the complainant in the following terms —

> *If within **48 HOURS** our client has not received payment, we will be given full instructions on the accounts. I would point out that once we have been instructed your name will be placed on our **CREDIT INFORMATION BUREAU.** This could affect your ability to obtain credit and loans from other companies.*

The first complainant was concerned that his personal details — including his unlisted telephone number — had been passed by the hospital to a third party, and he felt that this contravened the Act. The second complainant was very concerned that *"they will put me on a black list"*.

Section 2(1)(c) of the Data Protection Act provides *inter alia* that personal data —

> *(i) shall be kept only for one or more specified and lawful purposes, [and]*
>
> *(ii) shall not be used or disclosed in any manner incompatible with that purpose or those purposes.*

Section 1 of the Act defines "*disclosure"* in the following terms —

> *"disclosure", in relation to personal data, includes the disclosure of information extracted from such data and the transfer of such data but does not include a disclosure made directly or indirectly by a data controller or a data processor to an employee or agent of his for the purpose of enabling the employee or agent to carry out his duties ... .*

From my investigation of the case, I established that the debt collection service was retained by the hospital as its agent for the purpose of collecting outstanding moneys. I determined that the relationship between the hospital and the debt collection service was a *bona fide* principal-agent relationship, in that: (i) there was a formal contractual relationship in place between the hospital and the debt collection service; (ii) the contract made clear that the hospital retained control over the personal records in question; and (iii) the debt collection service was not permitted to retain the personal data for longer than necessary for the purpose of collecting the debt. Accordingly, I concluded that the Data Protection Act did not preclude the hospital from passing personal data, including patients' telephone numbers held by the hospital, to the debt collection agency.

On the question of the retention of personal details on the debt collection agency's files, my Office had detailed discussions with the debt collection agency. It was pointed out that the agency had no entitlement to retain personal details regarding the hospital's patients, and that it certainly had no entitlement to use these details to create a credit reference "blacklist". The agency explained that the language it used on its correspondence with debtors was designed to put maximum pressure on the

debtors to pay what they owed. However, I pointed out my view that it is not permissible for a debt collection agency, or indeed for any data controller, to misrepresent the purpose for which it keeps personal data, in order to put people under pressure to behave in a certain way. As a result of these discussions, the debt collection agency agreed to reword its letters so as to avoid any misrepresentation of what it is entitled to do with personal data it keeps as agent of the hospital. The managing director wrote to the complainants apologising for any inconvenience or distress caused, and confirming that the information had not been made available to any third party.

CASE STUDY 8 — telecommunications company - electronic publication of telephone directory on the Internet and CD-ROM - advanced and novel search capabilities - whether compatible with purpose for which data were obtained

A telecommunications company transferred the database of its telephone subscribers to a subsidiary company, which was tasked with arranging for publication of a telephone directory. The subsidiary published the directory in paper format and also in electronic format as a CD-ROM and, later, published the electronic directory on the Internet as well. Several individuals complained about the data protection implications of the electronic publication of the telephone directory. The complaints fell into the following two categories:

- Some people were unhappy that the telephone directory, which traditionally was published in paper format, should be made available in electronic format. These complainants had no objection to their details being available for manual searching, but considered that electronic publication was qualitatively different and was not something to which they had consented.
- Other people had no objection in principle to their data being available in electronic format, provided that the search capabilities of the electronic version were restricted to what was available in the manual directory. Their complaint was that the Internet directory was capable of being searched in completely new ways, which could undermine their privacy.

In data protection terms, the issue to be considered was whether the publication of the electronic directory, and the novel uses of personal data involved in such publication, were compatible with the purposes for which the personal data had been obtained and were kept by the data controller, as required by ***section 2(1)(c)(ii)*** of the Data Protection Act.

In considering whether a particular use of personal data is compatible with the purpose for which the data were obtained and kept, a useful question to ask is: what would a data subject have reasonably expected to happen to his or her data at the time the data were obtained? In the case of telephone directory information, the answer to this question is, in my view, that individuals would normally have expected their data to be made publicly available in the manual telephone book (unless, of course, they had expressed a preference for their telephone number to be ex-directory or unlisted). Many telephone subscribers, in my view, would not have been aware that an electronic version of the manual telephone directory existed, or would exist in the future. Does this imply that subscribers should have been asked for their consent before their details were included in the electronic directory? Having considered the matter in detail, I came to the view that if an individual was content to have his or her details included in a manual telephone directory (where the option not to do so was readily available), a telecommunications company was reasonably entitled to assume that the individual would not object to the same details being made available in electronic format. The electronic medium is simply one of a number of ways in which details can be made available publicly. Where appropriate safeguards are in place, electronic publication of itself need pose no additional risks to the privacy of the persons concerned.

However, to the extent that electronic publication is coupled with novel capabilities for the processing of personal data, then additional data protection issues arise for consideration. In the case in question, two distinct forms of processing could be identified for both the CD-ROM and Internet versions of the directory. First, the looking-up of a particular telephone directory entry based on the subscriber's name could be accomplished in a rapid fashion, by virtue of the computerised nature of the directory. I did not view this processing function as being novel, since this function simply replicated, in an efficient and convenient way, the traditional manner of looking up entries in a paper telephone directory. Second, the directory also facilitated the looking-up of subscriber details based on address. In other words, a particular address could be typed into the directory, without entering a subscriber name, and the directory would then show the name and telephone number of the subscriber at that address. Indeed, if a street name was entered, the directory would return a list of all the subscribers in that street, showing house numbers and telephone numbers.

In my view, this second processing capability was novel, since a traditional manual telephone directory could not be searched in this way. Some complainants made the point that this new search capability could have material consequences — for example, a burglar might use the reverse listings to obtain the telephone numbers for particular houses, and could call the telephone number for that address to confirm that no-one was home. In the light of such considerations, I concluded that subscribers could not reasonably be assumed to have consented to this new use of their personal data. Accordingly, I requested the telecommunications company to stop making the telephone directory available on the Internet, and to stop publishing the CD-ROM version pending discussions on the matter.

My Office had a productive dialogue with the telecommunications company, and the company agreed to modify significantly the electronic version of its directory. The modified electronic directory is now subject to the same search principles as the traditional manual directory, with some minor additions (such as the capability of searching names phonetically). Novel forms of searching, such as searching backwards from the address, are no longer possible.

Since this case was concluded, the Article 29 Group of EU Data Protection Commissioners has formalised its views on the general question of reverse telephone directories, reflecting significant input from my Office based on the Irish experience. The Article 29 Group's statement, due to be published shortly, affirms the principle that consent is required before a telecommunications company can subject its subscriber directory database to new search capabilities. The Group's statement also illustrates that lessons learned in the Irish context can positively influence the overall European environment for the protection of consumer privacy.

CASE STUDY 9 — Government Department - issue of request for tenders - inclusion of some personal data - whether data disclosed within meaning of the Act

A Government Department issued a request for tenders in connection with the administration of an official scheme. Included with the documentation issued by the Department was an extract from an administration database, giving a list of names of individuals who had benefited from the scheme, the county where each individual lived, and the amounts of money received by each individual. One of the persons who received the documentation was concerned about the data protection implications involved, and brought the matter to my attention for investigation. As this person was not an individual directly affected by the apparent disclosure of personal data by the data controller, I was not obliged to investigate the matter as provided for under ***section 10(1)(b)(i)*** of the Data Protection Act. However, I exercised my discretion under ***section 10(1)(a)*** to investigate the matter, as I was "*otherwise of opinion*" that a contravention of the Act might be involved if the alleged improper disclosure of personal data had in fact taken place.

My Office contacted the Department in question asking for their observations on the matter, having regard to ***section 2*** of the Act, which provides *inter alia* that personal data held by a data controller —

(i) shall be kept only for one or more specified and lawful purposes, [and]

(ii) shall not be used or disclosed in any manner incompatible with that purpose or those purposes.

The Department responded by admitting that its tender documentation did include the names of scheme beneficiaries, including the amounts of money received by those individuals. However, the Department argued that, since the individuals' addresses had not been made available, the individuals' identities could not have been determined by the tenderers.

Section 1(1) of the Act, in the definition of *"disclosure"*, provides that —

... where the identification of a data subject depends partly on the data and partly on other information in the possession of the data controller, the data shall not be regarded as disclosed unless the other information is also disclosed.

In the terms of the Act, therefore, the Government Department was arguing that the individuals could not be fully identified because only their names and county of residence, and not their addresses, had been made available; and since the individuals could not be fully identified, there was no "disclosure" as defined in the Act.

After some consideration, I was unable to accept the argument put forward by the Government Department. The first question I considered was what is normally meant when one speaks of "identifying" someone. To my mind, "identification" involves the process of distinguishing one particular person from another person, or from people generally. In everyday life, the chief method of distinguishing one person from another is by name. I am therefore most reluctant to accept that a data controller can release people's names and other data relating to those people, and still maintain that it has not disclosed personal data within the meaning of the Act. Moreover, since named individuals in this case were classified according to their county of residence, and since many of the names were uncommon, I was satisfied that a disclosure had clearly taken place. I also adjudged that the disclosure was not compatible with the purpose for which the Department had obtained the personal data, and accordingly I concluded that the Department had indeed contravened the Data Protection Act.

Data controllers in both the public and private sectors should be aware that, unless they have good grounds for making their customers' names available to third parties, they are likely to be in contravention of the Data Protection Act by doing so. Where, as in this case, a data controller can achieve its legitimate purposes without disclosing personal data, then, in my view, the only prudent approach is to avoid the unnecessary disclosure.

CASE STUDY 10 — identification of the data controller where control of database disputed - appeal from Decision of Data Protection Commissioner to Circuit Court

A number of individuals from a voluntary organisation ("V") contacted my Office to complain that another organisation ("S") was using V's database without authorisation. The database included names, addresses and highly sensitive personal information. The complainants, who were all data subjects on the database in question, requested that I immediately stop the allegedly unauthorised use of the data.

Having raised the matter with S, it quickly became apparent that there was a dispute as to which organisation was the lawful data controller of the database in question. Both parties agreed that another organisation ("D"), which was now disbanded, had at one time been the lawful data controller in respect

of the database. In view of the complexities of the case, and having regard to the sensitivity of the personal data in question, I informed S that it should refrain from using the data, over which it was in a position to exercise physical control, until the data protection issues were resolved. To address these issues, it was necessary to investigate how D came to be the data controller, and the circumstances in which it discontinued its operations.

A brief outline of the broad sequence of events is as follows. Several years previously, a Government Minister had established an ad-hoc group, "C", to lay the groundwork for the creation of the organisation, D, representative of a certain section of the public. C accepted application forms from people for inclusion on an electoral roll. These application forms provided the information from which the database was created. Persons, when completing the application form, were required to sign a declaration which included the following —

> *I understand my name will be entered on the electoral roll which will be maintained in the strictest confidence under the provisions of the Data Protection Act, 1988. I further understand and accept the electoral roll will be available to all local candidates for election in my county who might wish to canvass my support.*

D's constitution provided that it was established on an interim basis, with a fixed term of existence, during which it would prepare elections to a permanent body, E. It transpired, however, that D's management operations were beset with difficulties, and as the end of its term of existence approached, the objective of preparing elections to E seemed unattainable. The Minister then proposed that, after D's term of existence had expired, the task of arranging elections to E would pass to a new group, S. Some members of D were concerned at this arrangement. However, at its final annual general meeting, D gave qualified backing to the Minister's proposal. Alternative proposals to prolong D's lifespan to enable it to meet its original objectives were put to the annual general meeting and defeated.

S was duly established and carried on the functions of D, which was disbanded. Subsequently, however, some former members of D registered the organisation V as a limited company, using a similar title to that of the former organisation D. These people felt that V was the legitimate successor to D, and was therefore the only body entitled to use the membership database that had previously been controlled by D. These individuals also claimed that the qualifications which D had attached to its support for the establishment of S had not, in fact, been complied with by the Minister in setting up the new group.

From the data protection point of view, the issue was in my view straightforward. D had properly controlled the database, with the consent of the data subjects, for the primary purpose of organising elections. Any legitimate successor organisation, using the database for the same purposes, would in my view be entitled to be the data controller in respect of that database. Accordingly, the substantive issue to be determined was not primarily a data protection issue, but rather a factual and legal question as to the status of V versus that of S. The conclusion I reached, in all the circumstances of the case, was that S had the better claim to be the data controller in respect of the personal data in dispute and accordingly I rejected the complaint and gave a formal Decision to that effect.

Two of the complainants exercised their right to appeal my Decision to the Circuit Court, as provided for in ***section 26*** of the Act. The Court, having reviewed all aspects of the case, upheld my decision.

Number 25 *of* 1988

DATA PROTECTION ACT, 1988

AN ACT TO GIVE EFFECT TO THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA DONE AT STRASBOURG ON THE 28TH DAY OF JANUARY, 1981, AND FOR THAT PURPOSE TO REGULATE IN ACCORDANCE WITH ITS PROVISIONS THE COLLECTION, PROCESSING, KEEPING, USE AND DISCLOSURE OF CERTAIN INFORMATION RELATING TO INDIVIDUALS THAT IS PROCESSED AUTOMATICALLY. [13*th July*, 1988]

BE IT ENACTED BY THE OIREACHTAS AS FOLLOWS:

Preliminary

Interpretation and application of Act.

1.—(1) In this Act, unless the context otherwise requires—

"appropriate authority" has the meaning assigned to it by the Civil Service Regulation Acts, 1956 and 1958;

"back-up data" means data kept only for the purpose of replacing other data in the event of their being lost, destroyed or damaged;

"civil servant" has the meaning assigned to it by the Civil Service Regulation Acts, 1956 and 1958;

"the Commissioner" has the meaning assigned to it by *section 9* of this Act;

"company" has the meaning assigned to it by the Companies Act, 1963;

"the Convention" means the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data done at Strasbourg on the 28th day of January, 1981, the text of which is set out in the *First Schedule* to this Act;

"the Court" means the Circuit Court;

"data" means information in a form in which it can be processed;

"data controller" means a person who, either alone or with others, controls the contents and use of personal data;

INTRODUCTION

In the previous sections of this Report, I have given an account of the activities of my Office during 1999, and reported upon actual casework that may be of some general interest. In addition to these elements, I have traditionally taken advantage of the Annual Report to step back, as it were, from these operational matters, and present a more in-depth or reflective analysis of some "live" data protection issues. In this Part, I outline my views on data protection as it applies in the workplace, a topic on which an increasing number of data controllers and data subjects are seeking guidance. I also provide an overview of the credit referencing system as it operates in Ireland, to provide an insight into what is a poorly-understood but profoundly important element of the financial infrastructure of our society.

DATA PROTECTION IN THE WORKPLACE

I am receiving an increasing number of queries, from both employers and individual employees, regarding the collection and use of personal data for employment purposes and the application of data protection in the workplace. Two broad categories of query can readily be identified: (i) questions relating to the collection, use and retention of personal data with a high privacy content, such as health records, conviction data and employment performance data; and (ii) questions relating to the monitoring of the behaviour of employees, particularly through monitoring of employee e-mails and internet browsing habits. It may be useful to make some general observations on these issues in the interests of encouraging discussion by interested parties on what is likely to be an area of growing importance to both employers and employees and their representative bodies. It will also be noted that guidance and commentary on the issues are available from international sources, to which I will refer in the text below, and from an interesting body of case law that is emerging, notably in the USA.

OBTAINING AND KEEPING DATA ABOUT EMPLOYEES

Employers who keep personal data about their employees are, in common with all data controllers, bound by the provisions of ***section 2*** of the *Data Protection Act, 1988,* which requires *inter alia* that personal data: (i) be obtained and processed fairly; (ii) be kept only for one or more specified and lawful purposes; and (iii) be adequate, relevant and not excessive in relation to the specified purpose or purposes.

Fair Obtaining of Employee Data

The requirement in the Act that personal data be "fairly obtained" is deliberately expressed in very general terms, so as to allow of universal applicability of this data protection principle in various different circumstances. The task of determining how to meet the "fair obtaining" requirement in a particular employment context falls, in the first instance, to the particular employer, as data controller, who must bring his or her judgement and common sense to bear upon the matter. If an employee, as data subject, feels that the employer has misconstrued his or her obligations under the Act, then it is open to the employee to complain to me, whereupon I will review the matter independently. I recognise, of course, that applying a very general principle to a specific circumstance is not always straightforward, and my Office accordingly strives to provide whatever useful guidance it may, without prejudice to the rights of either the employer or the employee. In providing such advice, my Office would be strongly influenced by, for example, the Council of Europe's Recommendation on the protection of personal data used for employment purposes[1]. This provides, in respect of the collection of data, that —

[1] *Council of Europe Recommendation No. R (89) 2 on the Protection of Personal Data used for Employment Purposes:* adopted on 18 January 1989. The quoted text is from paragraphs 4.1-4.4 of the document.

- *Personal data should in principle be obtained from the individual employee. The individual concerned should be informed when it is appropriate to consult sources outside the employment relationship.*
- *Personal data collected by employers for employment purposes should be relevant and not excessive, bearing in mind the type of employment as well as the evolving information needs of the employer.*
- *In the course of a recruitment procedure, the data collected should be limited to such as are necessary to evaluate the suitability of prospective candidates and their career potential. In the course of such a procedure, personal data should be obtained solely from the individual concerned. Subject to the provisions of domestic law, sources other than the individual may only be consulted with his consent or if he has been informed in advance of this possibility.*
- *Recourse to tests, analyses and similar procedures designed to assess the character or personality of the individual should not take place without his consent or unless domestic law provides other appropriate safeguards. If he so wishes, he should be informed of the results of these tests.*

Relevance of Employee Data

In any employment context, the employer naturally needs to have certain details regarding his or her employees. These details would ordinarily relate to the employees' qualifications and competence to perform the job, their job record, and administrative matters such as holidays, sick leave and payroll. If an employer proposes to hold other types of personal data that do not fall easily into these categories, then the employer would face a more onerous task, in my opinion, in defending these data as being "relevant and not excessive" for the purpose of managing an employment relationship.

This is not to say that the matter is always clear-cut for employers. For example, I could certainly envisage cases in which aspects of an individual's conviction record might reasonably be requested by employers in certain sectors, such as childcare and the security industry. There will also be cases where an employer will need to keep health details about an employee at a level of detail which exceeds the norm because of the particular responsibilities entrusted to that employee — as in the case of a surgeon, for example. The general principle is clear, however; an employer needs clear objective grounds, that are related to the employment concerned, as a basis for lawfully keeping personal data about employees. This approach is, in my opinion, consistent with the International Labour Office guidance that —

(1) An employer should not collect personal data concerning a worker's:

(a) sex life;

(b) political, religious or other beliefs;

(c) criminal convictions.

(2) In exceptional circumstances, an employer may collect personal data concerning those in (1) above, if the data are directly relevant to an employment decision and in conformity with national legislation.[2]

The test of relevance is a primary consideration, and precedes consideration of other matters, such as whether the data have been "fairly obtained". The fact that an employer determines that certain personal data would be relevant to a particular employment context would not, of course, justify the employer in using unfair means to obtain the data.

[2] *Protection of Workers' Personal Data: an ILO Code of Practice*, International Labour Office, Geneva, 1997, ISBN 92-2-110329-3. The quoted text is from paragraph 6.5 of the document.

MONITORING OF EMPLOYEE E-MAILS AND WEB BROWSING

Perhaps the most frequently asked question in the context of employee privacy is whether employers are entitled to read the e-mails sent and received by employees, and to track employees' web browsing activity. In the absence of specific legislation dealing with this issue, my response to this general question is as follows.

On the one hand, an employer is entitled to exercise reasonable control and supervision over employees and their use of business resources. E-mail services, paid for by the employer, clearly constitute a business resource, and I would not interpret data protection law in a way which would prohibit an employer from openly exercising fair supervisory or control functions in this regard. Quite clearly employers are entitled to promulgate policies to protect their property and good name and to ensure that they do not become inadvertently liable for the misbehaviour of their employees.

On the other hand, employees retain privacy and data protection rights that must be respected by an employer. As the Council of Europe Recommendation referenced above notes —

> *Respect for the privacy and human dignity, in particular the possibility of exercising social and individual relations at the place of work, of the employee should be safeguarded in the collection and use of personal data for employment purposes.*

Much will depend on the culture of the particular employment in question when it comes to considering the application of the data protection principles set out in the Act to, for example, a complaint by an individual employee that his employer is in contravention of the Act. If a culture has developed within an organisation that is consistent with the use by employees of e-mail as a personal resource, then this consideration, in my view, may well circumscribe the freedom of action available to an employer who wishes to monitor employee e-mails. If employees have been using the company e-mail system for personal correspondence, with the tacit agreement of the employer, then I think it most unlikely that an employer may access those personal items of correspondence without contravening the Data Protection Act. The requirement at ***section 2(1)(a)*** of the Act that personal data be *"obtained and processed fairly"* in my view requires that, if employees use e-mail for personal purposes on the understanding that the confidential nature of these e-mails will be respected, then such e-mails should not be accessed by an employer except with the express permission of the employees concerned.

Perhaps the most useful piece of advice for employers is that it is always advisable to have a clear statement of company policy in regard to the use and confidentiality of e-mails. If an employer wishes to monitor e-mails sent or received using the organisation's equipment, then the employees should be fully apprised of this fact. If an employer wishes to change from a "relaxed" regime, in which the use of e-mail for personal purposes is permitted, to a more restrictive regime, in which all e-mails would be liable to be accessed by the employer, then the employer should advise the employees in advance of the change, and the employees should have an opportunity to delete any personal material from the employer's e-mail system.

Similar reasoning can be applied in regard to monitoring of the web browsing habits of employees. If an employer wishes to track an employee's web browsing activity, then the employee should know in advance about the employer's policy. Again, the ILO Code of Practice referenced above provides useful guidance in this regard. *Paragraph 6.14* of the Code provides as follows —

> *(1) If workers are monitored they should be informed in advance of the reasons for monitoring, the time schedule, the methods and techniques used and the data to be collected, and the employer must minimize the intrusion on the privacy of workers.*

(2) Secret monitoring should be permitted only:

(a) if it is in conformity with national legislation; or

(b) if there is suspicion on reasonable grounds of criminal activity or other serious wrongdoing.

(3) Continuous monitoring should be permitted only if required for health and safety or the protection of property.

CONCLUSIONS

Respecting the privacy of employees is an obligation for all employers. This principle is not incompatible with an employer's right to exercise control over the use of business resources. It is important, however, that in exercising this right, an employer should behave consistently and in an up-front manner. To begin with, an employer should ensure that the personal details kept regarding his or her employees are relevant to the employment context. Moreover, employers should note that surreptitious monitoring of personal e-mails would be exceedingly difficult to justify in data protection terms. Conversely, if an employer has laid down clear policy rules prohibiting the use of e-mail for personal purposes, and stating that all e-mails are liable to be monitored, then an employee will have considerable difficulty in demonstrating that his data protection rights have been infringed solely by virtue of his employers monitoring of e-mail to and from the workplace. Similar considerations would in my opinion apply to an assessment of an employer's monitoring of the internet browsing patterns of his employees.

As indicated at the outset, these are general and preliminary views in response to an increasing number of queries about data protection in the workplace. I would welcome observations and feedback on these issues from both individual employees and employers and their representative organisations. There may well be scope for the development by the representative groups of a code of practice, as provided for in ***section 13*** of the Act, to clarify and formalise the data protection requirements in respect of these matters. I am also aware that the issue of data protection in the employment context is now being examined by the EU Commission. My Office has contributed to preliminary discussions at EU level in this regard, along with the Department of Enterprise, Trade and Employment, and I look forward to an outcome which will further clarify and enhance the privacy environment for employees

CREDIT REFERENCING

For most people today, credit has become central to their way of life. There are very few who do not have some form of "credit agreement" — be it a mortgage, personal loan, leasing contract or hire-purchase agreement. An opinion survey, undertaken on my behalf in 1997, revealed that people attached the greatest importance to the privacy of their financial history and credit details. It is not surprising therefore that queries in relation to credit referencing and credit agencies feature high among the wide range of queries which my office receives.

The principal credit reference agency in Ireland is the *Irish Credit Bureau Limited* (ICB) which was established in 1965 by a number of financial institutions. The stated objectives of these institutions in establishing the ICB were —

to assist in lowering the cost of credit, enable faster decision making in the provision of credit, and aid in the avoidance of over-indebtedness of its members' customers.

Member Institutions of the Irish Credit Bureau Limited

ACC Bank	AIB Bank	AIB Finance & Leasing
AIB Credit Cards	Anglo Irish Bank .	The Associates
Bank of Ireland Bank	BOI Direct	Banking 365
Bank of Ireland Finance	Bank of Ireland Credit Cards	Bank of Scotland (Irl.)
Bord Gais Finance	BNP Capital Finance	Everyday Finance
First Active	Fiat Auto Financial Services	Ford Credit Europe
Friends First Finance	GE Capital Woodchester Bank	HFC Bank
ICC Finance	ICS B.S.	IIB Finance
Irish Nationwide B.S.	Irish Life & Permanent B.S.	Irish Permanent Finance
Lombard & Ulster Banking	MBNA International Bank	National Credit Finance
National Irish Bank	POS Finance	Premier Bank
Tesco Personal Finance	TSB Bank	Western Finance

Today, thirty-six financial institutions are registered members of ICB (see box above). The information which is held on the ICB database relates to credit agreements between these ICB members and their customers. A condition of such agreements is that the customer agrees that the financial institution may use the data supplied for the purpose of credit checking. Consequently, where an individual enters a credit agreement with an ICB member, details of the individual's performance in complying with the terms of the agreement are input to the ICB "credit file" database, which may be accessed by all member institutions of ICB. Each time a person applies for credit from an ICB member, that institution accesses the ICB's "credit file" to ascertain the applicant's performance under any previous credit agreements with ICB members.

A measure of the scale and significance of the credit referencing system in Ireland is the fact that, at present, ICB holds 2.7 million names and addresses on its "credit file" database. The Data Protection Act provides data subjects with important rights to ensure that their data are accurate and are used appropriately. However, for individuals to be in a position to exercise these rights effectively, they naturally need to be conscious of the degree to which their personal data are being kept, and to have some practical understanding of how the credit referencing system operates. On the following two pages, I have reproduced, for illustrative purposes, a sample "credit file" record showing the credit history of a fictitious individual. This is the type of record an individual would receive from ICB in response to an access request under the Data Protection Act. An explanation of how this technical record is to be interpreted is given on page 38. I am glad to acknowledge the assistance of ICB in preparing this explanatory material.

SAMPLE "CREDIT FILE" RECORD

Note: This is a fictitious record, and the financial institutions mentioned have been selected randomly, for illustrative purposes. There is no suggestion that an actual record identical to this is kept by the Irish Credit Bureau.

IRISH CREDIT BUREAU LIMITED **Results of Own Enquiry**

A. Identification Details: **JOSEPH P. BLOGGS**
Customer Number: YY123456789 Occupation: OFFICE ADMINISTRATOR
Address: Irish Life Centre,
Dublin
Date of birth: 02/07/55

B. Details have been filed on the following transactions:

Account No: BI987654321
Open Date: 01/06/95 Financial Institution: Bank of Ireland
Reference Number: ZZ12345 Amount Financed: £15,000
Finance Type: LEASING CONTRACT Repayment Period(in months) 048
Association with account: INDIVIDUAL
Settlement Date: 31/05/99 Payment Performance: *1

Account No: AI876954321
Open Date: 05/07/95 Financial Institution: Allied Irish Bank
Reference Number: XX31245 Amount Financed: £30,000
Finance Type: Personal Loan Repayment Period(in months) 60
Association with account: INDIVIDUAL
Balance Date: 30/06/00 Balance Amount 0.00
Payment Frequency: Month Payment Profile: #C00000000000054333321110

Account No: LU123876954
Open Date: 10/02/95 Financial Institution: Lombard & Ulster
Reference Number: YY45312 Amount Financed: £10,000
Finance Type: Hire Purchase Repayment Period(in months) 37
Association with account: JOINT ACCOUNT
Balance Date: 31/03/99 Balance Amount 0.00
Payment Frequency: Month Payment Profile: #LPPPPPP5421000011133121

Account No: NI123876954
Open Date: 05/09/98 Financial Institution: National Irish Bank
Reference Number: UU45123 Amount Financed: £50,000
Finance Type: Mortgage Repayment Period(in months) 37
Association with account: INDIVIDUAL
Balance Date: 31/05/00 Balance Amount 35,700.00
Payment Frequency: Month Payment Profile: #000000022210000321000000

SAMPLE “CREDIT FILE” RECORD

CONTINUED

C. *Explanation of Performance Codes:

1 = Kept to terms
2 = Not kept strictly to terms
3 = Not kept to terms but completed
4 = Not kept to terms
5 = Settled early within terms
C = Current-Recently confirmed
? = Code sought on given date, still awaited

D. #Explanation of Profile Codes: (most recent code first)

0-9 = Number of payments in arrears
C = Completed Account
B = Borrower cannot be located by lender
P = Pending Litigation
G = Goods in merchantability Dispute
M = Moratorium
L = A/C settled for less than full amount
N = Non-active account
R = Repossession of goods
S = Surrender of goods
T = Terms revised
W = Element written off
Z = No further data updates available
- = No history reported

E. The following enquiries on your record were made recently:

Date	Time	Financial Institution	Enquiry Mode
03/01/99	1554	IRISH NATIONWIDE B.S.	Communications
16/03/99	0943	MBNA INT’L BANK	Communications
12/05/99	1137	TSB BANK	Dial-Up
08/06/99	1554	BORD GAIS FINANCE	Communications
20/06/99	0943	FIAT AUTO FIN. SERVICES	Communications
12/08/99	1623	PREMIER BANK	Communications
21/09/99	1216	BANKING 365	Dial-Up
14/11/99	1137	FORD CREDIT EUROPE	Dial-Up
07/01/00	1043	FIRST ACTIVE	Communications
07/03/00	1554	AIB CREDIT CARDS	Communications
11/04/00	1211	BANK OF SCOTLAND (IRELAND)	Dial-Up
20/06/00	0943	TESCO PERSONAL FINANCE	Communications

UNDERSTANDING YOUR ICB RECORD

The sample "credit file" gives a number of different profiles for individual accounts, showing the performance of the borrower in making repayments for each of the previous 24 months. The *Payment Profile* is the key indicator of performance. The profile is read from right to left, with the most recent indicator on the left. One of the profiles from the sample record reads as follows —

```
Payment Profile:  # C000000000000543333211l0
```

This profile indicates that, twenty-four months previously, there were no arrears on this particular account. The account subsequently deteriorated, rising to a peak of five monthly payments in arrear. However, the account was ultimately satisfactorily cleared (as indicated by the final code letter "C"). Another account on the sample record includes the following profile —

```
Payment Profile:  # LPPPPPP54210000111331211
```

This profile indicates that, twenty-four months previously, there was one monthly payment in arrear. The profile shows that repayments on the account were patchy and erratic, rising to five monthly payments in arrear, giving rise to litigation ("P" denotes Litigation Pending). The account was ultimately settled for less than the full amount (as indicated by code letter "L").

Another of the accounts in the sample file, while having a relatively solid payment profile with no current arrears, shows an outstanding balance of £37,700. Individuals should note that financial institutions pay particular attention to the *Payment Profile* and *Balance Amount* when considering applications for credit.

ACCESSING YOUR ICB RECORD

Section 4 of the *Data Protection Act, 1988*, provides a general "right of access" for an individual to all information kept about him or her on computer. A person wishing to avail of this provision to access their ICB credit record should contact the ICB at the address —

Irish Credit Bureau, Newstead, Clonskeagh Road, Dublin 14. Tel. (01) 260 0388

When making an access request to the ICB or to any data controller, a person should supply such information as the data controller may reasonably require to satisfy itself of the person's identity (e.g. name, address, customer account number) and to assist it in locating relevant data held. It is the practice of ICB, when processing access requests under section 4 of the Act, to request individuals to complete a standard access application form, which may be obtained by telephoning ICB at the number given above. I understand that the total number of access requests which ICB have received to date is about 47,000. The current level of access requests made to ICB is between 800 and 900 per month.

From time to time my Office receives data protection complaints involving ICB. These complaints generally centre on the accuracy of the information held on the ICB database, apparent failure to fully comply with an access request or alleged inappropriate disclosure of personal details. In some cases, it is the financial institution which has reported the data to ICB, rather than ICB itself, that is found to be at fault. On investigation of complaints involving ICB, it has been my experience that ICB, as a data controller, makes every effort to comply fully with its obligations under the Data Protection Act. In any instance where it has been necessary to take remedial action on foot of a complaint, ICB has responded positively and promptly.

Number 25 *of* 1988

DATA PROTECTION ACT, 1988

AN ACT TO GIVE EFFECT TO THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA DONE AT STRASBOURG ON THE 28TH DAY OF JANUARY, 1981, AND FOR THAT PURPOSE TO REGULATE IN ACCORDANCE WITH ITS PROVISIONS THE COLLECTION, PROCESSING, KEEPING, USE AND DISCLOSURE OF CERTAIN INFORMATION RELATING TO INDIVIDUALS THAT IS PROCESSED AUTOMATICALLY. [13*th July*, 1988]

BE IT ENACTED BY THE OIREACHTAS AS FOLLOWS:

Preliminary

Interpretation and application of Act.

1.—(1) In this Act, unless the context otherwise requires—

"appropriate authority" has the meaning assigned to it by the Civil Service Regulation Acts, 1956 and 1958;

"back-up data" means data kept only for the purpose of replacing other data in the event of their being lost, destroyed or damaged;

"civil servant" has the meaning assigned to it by the Civil Service Regulation Acts, 1956 and 1958;

"the Commissioner" has the meaning assigned to it by *section* 9 of this Act;

"company" has the meaning assigned to it by the Companies Act, 1963;

"the Convention" means the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data done at Strasbourg on the 28th day of January, 1981, the text of which is set out in the *First Schedule* to this Act;

"the Court" means the Circuit Court;

"data" means information in a form in which it can be processed;

"data controller" means a person who, either alone or with others, controls the contents and use of personal data;

Appendix 1

SELECTED DOCUMENTS ADOPTED BY THE EU DATA PROTECTION WORKING PARTY (ARTICLE 29 GROUP)

The Working Party established under ***Article 29*** of the EU *Directive 95/46/EC* is composed of representatives of the Data Protection Commissioners from all the EU Member States, along with an EU Commission representative. The Working Party is an independent body, and it considers data protection matters of relevance throughout the EU. The work of the Group serves to promote consistency and uniformity of approach to dealing with data protection matters across the various jurisdictions. The documents adopted by the Working Party express authoritatively the views of the EU's Data Protection Commissioners, and it is therefore advisable that data controllers should take the recommendations of the Working Party fully into account when formulating and reviewing policies and procedures regarding personal data.

The list below gives a selection of documents from the Working Party that may be of interest to data controllers and data subjects in Ireland. The texts of documents of particular relevance to current issues are reproduced in full in Appendices 3 - 5. A full listing of the Article 29 Working Party documents, together with the full texts, can be obtained on the EU Commission's web site at the following address:

http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm

Reference	Document	Date
5012/97	Recommendation 1/97: Data protection law and the media	25/02/97
5060/97	Recommendation 2/97: Report and Guidance by the International Working Group on Data Protection in Telecommunications ("Budapest — Berlin Memorandum on Data Protection and Privacy on the Internet")	03/12/97
5022/97	Recommendation 3/97: Anonymity on the Internet	03/12/97
5005/98	Working Document: Preliminary views on the use of contractual provisions in the context of transfers of personal data to third countries	22/04/98
5009/98	Recommendation 1/98 on Airline Computerised Reservation	28/04/98
5032/98	Opinion 1/98: Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS)	
5025/98	Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive	24/07/98
5013/98	Working Document: Processing of Personal Data on the Internet	23/02/99

5093/98	Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet performed by Software and Hardware	23/02/99
5005/99	Recommendation 2/99 on the respect of privacy in the context of interception of telecommunications	03/05/99
5026/99	Opinion 3/99 on Public Sector Information and Data Protection	03/05/99
5085/99	Recommendation 3/99 on the preservation of traffic data by Internet Service Providers for law enforcement purposes *(see full text in Appendix 4 of this Report)*	07/09/99
5143/99	Recommendation 4/99 on the inclusion of the fundamental right to data protection in the European catalogue of fundamental rights *(see full text in Appendix 5 of this Report)*	07/09/99
5007/00	Opinion 1/2000 on certain data protection aspects of electronic commerce *(see full text in Appendix 2 of this Report)*	03/03/00
5009/00	Opinion 2/2000 concerning the general review of the telecommunications legal framework *(see full text in Appendix 3 of this Report)*	03/03/00
5139/00	Recommendation 1/2000 on the Implementation of Directive 95/46/EC	03/02/00
CA07/434/00	Opinion 4/2000 on the level of protection provided by the "Safe Harbor Principles"	16/05/00

Appendix 2

ARTICLE 29 DATA PROTECTION WORKING PARTY

OPINION 1/2000

ON CERTAIN DATA PROTECTION ASPECTS OF ELECTRONIC COMMERCE

Presented by the Internet Task Force

1. Introduction

The EU is currently in the process of adopting a proposal for a directive on certain legal aspects of e-commerce[1]. As it has done to date, the Article 29 Data Protection Working Party[2] intends to make a constructive input into this reinforcement of the legal framework for e-commerce. With this Opinion, the Working Party intends to highlight a data protection issue raised by e-commerce, and to explain how it is dealt with in the European legislation. The legal framework for the protection of the fundamental right to privacy and the protection of personal data is already in place in form of Directive 95/46/EC laying down the general data protection principles and in form of Directive 97/66/EC supplementing them for the telecommunications sector.

The Working Party would like to express its satisfaction that the text currently in the process of adoption now contains express clarification, in a new recital and a new article 1(4)(b), as to the full and proper application of the data protection legislation[3] to internet services. This means that the implementation of the e-commerce directive must be completely in line with data protection principles.

The Working Party has already given considerable attention to internet-related data protection issues, most notably in 1999 by issuing general guidance on three important questions related to the specific characteristics of new information technologies. It has issued an opinion on public sector information[4], and recommendations on invisible and automatic processing of personal data on the internet[5], and the

[1] Amended proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the internal market, COM (1999) 427 final. Political agreement on a text was reached in the Council of Ministers on the 7th December 1999; a Common Position will soon be formally adopted before a second reading at the European Parliament. See Press Release IP/99/952. p.1 and 4

[2] Established by article 29 of Directive 95/46/EC, cited in footnote 3 below

[3] Directive 95/46/EC of the European Parliament and the Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, JO L 281/31 of 23rd November 1995, and Directive 97/66 of the European Parliament and of the Council of 15th December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, JO L 24/1 of 30th January 1998, both available at http://europa.eu.int/comm/internal_market/en/media/dataprot/law/index.htm

[4] Opinion 3/99 on Public Sector Information and the Protection of Personal Data, adopted on 3rd May 1999: WP 20 (5055/99). All documents adopted by the Working Party are available at: http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm

[5] Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet performed by Software and Hardware, adopted on 23rd February 1999: WP 17 (5093/98)

preservation of traffic data by internet service providers for law enforcement purposes[6]. In the context of e-commerce, a fourth question arises. The Working Party would now like to give an interpretation on the application of European data protection rules to data processing for electronic mailing purposes.

2. The issue of electronic mailing

In order to launch an advertising campaign or commercial mailing, a company must acquire an extensive and appropriate list of e-mail addresses of potential customers. There are three possible ways in which companies can acquire e-mail addresses from the internet : direct collection from customers or visitors of web sites; lists prepared by third parties[7]; and collection from internet public spaces such as public directories, newsgroups or chat-rooms.

A particular feature of electronic commercial mailings is that while the cost to the sender is extremely low compared to traditional methods of direct marketing, there is a cost to the recipient in terms of connection time. This cost situation creates a clear incentive to use this marketing tool on a large scale, and to disregard data protection concerns and the problems caused by electronic mailing.

The problem from the citizen's point of view is threefold : firstly, the collection of one's e-mail address without one's consent or knowledge; secondly, the receipt of large amounts of unwanted advertising; and thirdly, the cost of connection time. A leading issue in this field is spam[8]. Spamming is the practice of sending unsolicited e-mails, usually of a commercial nature, in large numbers and repeatedly to individuals with whom the sender has no previous contact. It typically occurs when an e-mail address has been collected in a public space on the internet. The problem from an internal market point of view is the possibility of divergent national regulation of electronic commercial communication creating barriers to trade. Both types of problem have been influential in the development of relevant Community legislation.

3. Community legislation and its application to electronic mailing

The general point has already been made that data protection legislation applies to e-commerce[9]. Electronic mailing is a specific example of how the data protection problems raised by e-commerce can be resolved using the legal principles contained in the two directives. The general directive states that personal data must be collected fairly, for specified, explicit and legitimate purposes, and processed in a fair and lawful manner in line with those stated purposes[10]. Processing must take place on legitimate grounds such as consent, contract, law or a balance of interests[11]. Furthermore the individual has to be informed about intended processing[12], and given the right to object to processing of their personal data for direct marketing purposes[13]. The telecommunications privacy directive gives Member States the

6 Recommendation 3/99 on the preservation of traffic data by internet service providers for law enforcement purposes, adopted on 7th September 1999 : WP 25 (5085/99)

7 The lists prepared by a third party may be established on the basis of data collected directly from customers or on the basis of data collected in internet public spaces. This subject has been dealt with by the Report on Electronic Mailing and Protection of Personal Data adopted by the CNIL on October 14th 1999, available at www.cnil.fr. Parts 2 and 3 of this Opinion are based to some degree on that Report.

8 This subject has been dealt with by the Report on Electronic Mailing and Protection of Personal Data adopted by the CNIL on October 14th 1999, available at www.cnil.fr. Parts 2 and 3 of this Opinion are based to some degree on that Report.

9 Working document: Processing of Personal Data on the Internet. Adopted on 3.2.1999: WP 16 (5013/99)

10 Directive 95/46/EC, article 6

11 Directive 95/46/EC, article 7

12 Directive 95/46/EC, article 10

13 Directive 95/46/EC, article 14

choice between applying “opt-in” and “opt-out” rules for unsolicited commercial communications[14]. To the data protection rules are added certain requirements inspired by consumer protection. The distance selling directive requires for example that consumers as a minimum be given the right to object to distance communication[15] operated by means of e-mail.

The e-commerce directive may, once adopted, make explicit provision in article 7 on two technical aspects : the obligation to identify commercial e-mail as such, and the obligation to consult and respect opt-out registers where they are provided for by national rules. But a recital and article 1(4)(b) make it clear that this directive is in no way intended to change the legal principles and requirements contained in the existing legislative framework outlined above. Since the data protection legislation fully applies to e-commerce, the implementation of the e-commerce directive must be completely in line with data protection principles. This means firstly that as far as data protection is concerned, the national law applicable to a company responsible for the processing of personal data will continue to be that of its country of establishment in EU[16]. It also means that the e-commerce directive could neither prevent Member States from requiring companies to seek prior consent for commercial communications[17], nor the anonymous use of the internet[18].

In the view of the Working Party, these rules provide a clear answer to the privacy issues raised in part 2 above, and give a clear picture of the rights and obligations of those involved. Two situations should be distinguished :

- If an e-mail address is collected by a company directly from a person with a view to electronic mailing by that company or a third party to which the data are disclosed, the original company must inform the person of those purposes at the time of collecting the address[19]. The data subject must also, as a bare minimum, be given at the time of collection and at all times thereafter the right to object to this use of his data by easy electronic means, such as clicking a box provided for that purpose, by the original company and further on by the companies which have received data from the original company[20]. Certain national laws implementing the relevant directives even require the company to obtain the data subject’s consent. The requirements of the draft e-commerce directive’s article on unsolicited commercial communications would complement these rules at a technical level by imposing the obligation to consult a register on the service provider, but would not take anything away from the general obligations applicable to data controllers.
- If an e-mail address is collected in a *public space on the internet*¸ its use for electronic mailing would be contrary to the relevant Community legislation, and this for three reasons. Firstly, it could be seen as “unfair” processing of personal data in terms of article 6(1)(a) of the general directive. Secondly, it would be contrary to the purpose principle of article 6(1)(b) of that directive, in that the data subject made his e-mail address public for quite a different reason, for example participation in a newsgroup.

14 Directive 97/66, article 12. It could even be argued that the use of e-mail for direct marketing is to be considered equivalent to the use of automated calling devices which does require consent of the data subject.

15 Directive 97/7/EC of the European Parliament and of the Council of 20th May 1997 on the protection of consumers in respect of distance contracts, OJ L 144/19 of 4th June 1997, article 10 (e-mail is expressly included in this by means of article 2(4) and annex 1); available at http://www.europa.eu.int/eur-lex/en/lef/dat/1997/en_397L0007.html

16 Directive 95/46/EC, article 4.

17 See article 12 of directive 97/66/EC

18 See recital 6a of the amended proposal, footnote 1 above

19 Directive 95/46/EC, article 10

20 Directive 95/46/EC, article 14

Thirdly, given the cost imbalance and the disruption to the recipient, such mailing could not be regarded as satisfying the balance of interest test of article 7(f)[21].

4. Conclusions

This Opinion is not intended as the final position of the Working Party on the interaction between e-commerce and data protection. Its objective is to raise awareness of the issues raised by a particular type of data processing which is currently the subject of debate in many circles, and to contribute to understanding of the legal framework applicable to e-commerce. There may well be other e-commerce issues beyond those already dealt with by the Working Party that may require interpretative guidance or a common approach. Therefore the Working Party considers it necessary to develop a common policy on aspects ranging from cyber-marketing to electronic payments, to Privacy Enhancing Technologies. It has mandated its Internet Task Force to continue this work. Various outcomes are expected, including recommendations on technical measures related to spam, or the validation of web sites according to a common European checklist based on the data protection directives.

Done at Brussels, 3 February 2000

For the Working Party

The Chairman

Peter J. HUSTINX

[21] That provision (one out of several possible legitimate grounds for processing) requires data processing to be "necessary for the purposes of legitimate interests pursued by the controller . . . except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject".

Appendix 3

ARTICLE 29 DATA PROTECTION WORKING PARTY

OPINION 2/2000

CONCERNING THE GENERAL REVIEW OF THE TELECOMMUNICATIONS LEGAL FRAMEWORK

Presented by the Internet Task Force

1. Introduction

The Working Party for the Processing of Personal Data[1] has taken notice of the Communication of the European Commission[2] concerning the general review of the existing telecommunications legal framework at European level.

In the context of the public consultation opened by the European Commission until the 15th of February 2000, the Working Party wishes to highlight the importance of the data protection issues raised in this context. Furthermore, the Working Party wants to manifest its wish to be involved and to make a constructive input into the revision of the legal framework for telecommunications.

2. Relevant data protection issues in the context of the general review

Within the framework of the envisaged general review of the telecommunications legal framework, the existent directive concerning the processing of personal data and the protection of privacy in the telecommunications sector[3] will also be revised and updated. Article 14 paragraph 3 of this directive mandates the Working Party established by Directive 95/46/EC to carry out its tasks also with regard to the protection of fundamental rights and freedoms and of legitimate interests in the telecommunications sector which is subject of Directive 97/66EC. Article 30 of the general data protection directive deals with the tasks of the Working Party. One of its tasks is to advise the European Commission on any proposed amendment of the directive or any additional or specific measures to safeguard the rights of freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms.

In previous opinions of this group, the Working Party has already underlined the necessity of taking into account new technological developments[4], which could present a challenge for the protection of

[1] Established by article 29 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, JO L 281, 23 November 1995, p. 31. Available at: http://europa.eu.int/comm/dg15/en/media/dataprot/law/index.htm

[2] Document COM (1999) 539.

[3] Directive 97/66/EC of 15 December 1997, Official Journal L 24, Volume 41of 30 January 1998.

[4] Among others, in the Working Document Processing of Personal Data on the Internet, adopted on 23 February 1999, document 5013/99/EN/final Working Party 16. All documents adopted by the Working Party are available at: http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/index.htm

personal data and the right to privacy. In this sense, the Working Party welcomes an update of this directive in so far as this allows it to address in a more specific way the data protection issues in the telecommunication sector while maintaining or, where necessary, improving the existing level of protection. It should however not be forgotten that the specific directive 97/66/EC only complements the general directive 95/46/EC by establishing specific legal and technical provisions[5].

When revising the specific directive, it will be necessary to take into account, respect and be coherent with the provisions of the general data protection directive 95/46/EC, that applies to any processing of personal data falling under its scope, irrespective of the technical means used. The specific directive should obviously not only protect the fundamental rights of individuals but should as well take into account other legitimate interests, such as the ones of the confidentiality and integrity of public telecommunications.

The text of the Communication of the European Commission points out that the envisaged review will pay special attention to the terminology used by directive 97/66/EC in order to make clear that new services and technologies are covered by this directive, avoiding in this way possible ambiguities and facilitating a consistent application of the data protection principles. The Working Party welcomes such a re-examination of the terminology for these purposes.

As it is correctly stated in the Communication of the European Commission, the telecommunication legal framework should apply to Internet services in the same way as it applies to other forms of communication. The Working Party has already addressed this issue in precedent opinions and has clearly stated that processing of personal data on the Internet has to respect data protection principles just as in the off-line world[6]. Personal data processing on the Internet therefore has to be considered in the light of both data protection directives. The Working Party, and in particular the Internet Task Force created within this group, would like to offer its specific data protection expertise to the Commission for the Internet-related issues which should be dealt with in the framework of the general review of the telecommunications legislation.

Another interesting issue addressed in the Commission's communication is the growing impact of software and software-driven configurations of technology. The Working Party has already dedicated some attention to this question in the past, in particular in its recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware[7]. In this recommendation, the Working Party encouraged the software and hardware industry to work on Internet privacy-compliant products that provide the necessary tools to comply with the European data protection rules. The Working Party thinks that the increasingly bigger role of software in the telecommunications field should be taken into account in the revision of this directive, especially when dealing with the responsibilities of all actors involved in the data processing operations. The revision of the directive could also be a good opportunity to reconsider the different responsibilities that network operators and service providers should have in this field.

One of the objectives of the revision of legislative framework for telecommunications is to develop European legislation in a technology-neutral direction. The Working Party agrees with this objective. This intention should however not prevent the European legislator from producing a new legal

[5] To all matters which are not specifically covered by Directive 97/66/EC, such as the obligations on the controller and the rights of individuals or non-publicly available telecommunications services, Directive 95/46/EC applies (see recital 11 of Directive 97/66/EC).

[6] See also Ministerial Declaration of the Bonn Conference on Global Networks, June 1997, available at : http://www2.echo.lu/bonn/conference.html.

[7] Recommendation 1/99, adopted by the Working Party on 23 February 1999, document 5093/98/EN/final Working Party 17.

framework that sufficiently addresses the specific issues raised by new technological developments in this field. It would also like to stress that a new directive in this field should emphasise that all technologies, irrespective of the kind of technical means used, should be privacy-compliant and, where possible, privacy-protective.

3. Conclusion

In general terms, the Working Party welcomes an update of directive 97/66/EC in so far as this update allows the directive to address in a specific way the data protection issues in the telecommunication sector while maintaining or, where necessary, improving the existing level of protection. The Working Party attaches great importance to a high level of data protection in the telecommunications sector and, in particular, to guaranteeing the confidentiality and integrity of the communications.

While favouring an update and improvement of the telecommunications legal framework, the Working Party would like to underline the importance of a timely implementation of the current directive in the telecommunication sector at national level. The Group would therefore invite the Commission to make clear in its communications that the new legal framework will only be in place within a number of years and that, in the meantime, Member States should continue drafting their national legislation within the existing legal framework.

The Working Party would like to encourage the Commission in taking into account all recommendations, opinions and working documents drafted by this Working Party which refer to the issues addressed in its communication in the revision process.

This Opinion is in no way intended to be the final position of the Working Party on the issue. The Working Party wishes to contribute to the further discussion of this subject and to provide specific suggestions, if so wished, for the next steps of the revision procedure.

Done at Brussels, 3 February 2000

For the Working Party

The Chairman

Peter J. HUSTINX

Appendix 4

ARTICLE 29 DATA PROTECTION WORKING PARTY

RECOMMENDATION 3/99

ON THE PRESERVATION OF TRAFFIC DATA BY INTERNET SERVICE PROVIDERS FOR LAW ENFORCEMENT PURPOSES

Introduction

Combating computer-related crime is an issue that has been acquiring increasing international attention[1]. The G8 countries[2] have adopted a 10 point action plan[3] which is currently being implemented with the help of a specialised high-tech crime subgroup consisting of representatives G8 law enforcement agencies. One of the outstanding and most controversial issues is the preservation of historic and future traffic data by Internet Service Providers for law enforcement purposes and disclosure of such data to law enforcement authorities. The G8 high-tech crime subgroup intends to propose recommendations to ensure the possibility of preserving and disclosing traffic data. G8 Ministers of Justice and Home Affairs may discuss these recommendations in a meeting in Moscow on 19 - 20 October 1999.

The Working Party on the Protection of Individuals with regard to the Processing of Personal Data[4] is conscious of the important role that traffic data can play in the context of the investigation of crimes perpetrated over the Internet but wishes however to remind the national governments about the principles on the protection of the fundamental rights and freedoms of natural persons, and in particular of their privacy and the secrecy of their correspondence which need to be taken into account in this context.

The Working Party has understood that the G8 Justice and Home Affairs Ministers may be asked to call for a balanced interpretation of the two EU Data Protection Directives[5] at the stage of implementation that will take into account law enforcement interests alongside privacy interests.

---

[1] See for example “COMCRIME Study -Legal Aspects of computer-related Crime in the Information Society” - COMCRIME Study, January 1997 - Delivered within the EU Action Plan on organised crime - Available on the Legal Advisory Board Website: http://www2.echo.lu/legal/en/comcrime/sieber.html. The Council of Europe is working on an draft convention on cyber-crime. The EU Council has expressed its support for this work on 27 May 1999. Computer related crim refers to all crimes committed over networks such as computer attacks, publication of illegal material on web sites, including criminal activity committed by transnational organised crime (e.g. narcotics traffickers, child pornographers).

[2] G8 countries are: Canada, France, Germany, Italy, Japan, the United Kingdom, United States of America and Russia.

[3] “Meeting of Justice and Interior Ministers of the Eight December 9-10, 1997, Communiqué, Washington D.C. December 10, Communiqué Annex: Principles and Action Plan to Combat High-tech Crime”.

[4] Instituted by Article 29 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281 of 23.11.1995, p. 31. Available at: http://europa.eu.int/comm/internal_market/en/media/dataprot/law/index.htm

[5] Directive 95/46/EC see footnote 3 and Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, OJ L 24, 30 January 1998, p.1. Available at: see footnote 4.

The Working Party is also conscious of the burdens that may be put on telecommunication operators and service providers.

The objective of the present Recommendation is therefore to contribute to an uniform application of Directives 95/46/EC and 97/66/EC with a view to providing for clear and predictable conditions for telecommunications operators and Internet Service Providers as well as for law enforcement authorities whilst preserving the right to privacy.

Legal situation

Within the European Union, Directive 95/46/EC harmonises the conditions of the protection of the right to privacy enshrined in the legal systems of the Member States. This Directive gives substance to and amplifies the principles contained in the European Convention for the Protection of Human Rights of 4 November 1950 and in Council of Europe Convention No. 108 of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data. Directive 97/66/EC particularises the provisions of this Directive in the telecommunications sector. Both Directives apply to processing of personal data, including traffic data related to subscribers and users, on the Internet[6].

In particular Articles 6, 7, 13, 17 (1) and (2) of Directive 95/46/EC and Articles 4, 5, 6 and 14 of Directive 97/66/EC deal with the lawfulness of such processing by telecommunication operators and service providers.

These provisions allow telecommunications operators and telecommunications service providers to process data on telecommunications traffic under certain very limited conditions.

Article 6 (1) lit. b) provides that data may only be collected for specified, explicit and legitimate purposes and not further processed in a way which is incompatible with the purposes for which the data were collected. Article 6 (1) lit. e) provides that personal data must not be kept longer than is necessary for the purposes for which the data were collected or for which they are further processed. Article 13 allows Member States to restrict the scope of inter alia Article 6 (1) insofar such restriction constitutes a necessary measure to safeguard national security, public security or the prevention, investigation, detection and prosecution of criminal offences.

The application of these principles is further specified in Article 5 and Article 6 paragraphs 2 to 5 of Directive 97/66/EC. Article 5 guarantees the **confidentiality of communications** by means of a public telecommunications network and publicly available telecommunications services. Member States have to prohibit the listening, tapping, storage or other kinds of interception or surveillance of communications by others than users, without the consent of the users concerned, except when legally authorised in accordance with Article 14 (1).

As a general rule, **traffic data** must be erased or made anonymous as soon as the communication ends (Article 6 paragraph (1) of Directive 97/66/EC). This is motivated by the sensitivity of traffic data revealing individual communication profiles including information sources and geographical locations of the user of fixed or mobile telephones and the potential risks to privacy resulting from the collection, disclosure or further uses of such data. .Exception is made in Article 6 (2) concerning the processing of certain traffic data for the purpose of subscriber billing and interconnection payments, but only up to the end of the period during which the bill may lawfully be challenged or payment may be pursued.

Article 14 (1) allows Member States to restrict the scope of obligations and rights provided for in Article 6 when such restriction constitutes a necessary measure to safeguard national security and the

[6] See “Working document: Processing of Personal Data on the Internet”, adopted on 2nd February 1999, available at: see footnote 1.

prevention, investigation, detection and prosecutions of criminal offences as referred to in Article 13 (1) of Directive 95/46/EC.

It follows from these provisions, that telecommunications operators and Internet Service providers are not allowed to collect and store data for law enforcement purposes only, unless required to do so by law based on the reasons and under the conditions mentioned above. This is in agreement with longstanding traditions in most Member States, where the application of national data protection principles has resulted in a prohibition for the private sector to keep personal data on the sole basis of potential further need expressed by police or state security forces.

In this context it can be noted that for the purposes of law enforcement and under the conditions contained in Articles 13 of Directive 95/46/EC and Article 14 of Directive 97/66/EC, legislation exists in most Member States defining the precise conditions under which police and state security forces may have access to data stored by private telecommunications operators and Internet Service providers for their own civil purposes.

As the Working Party already stated in its Recommendation 2/99 on the respect of privacy in the context of interception of telecommunications adopted on the 3 of May 1999[7], the fact that a third party acquires knowledge of traffic data concerning the use of telecommunication services has generally been considered as a telecommunication interception and constitutes therefore a violation of the individuals' right to privacy and of the confidentiality of correspondence as guaranteed by Article 5 of directive 97/66/EC[8] . In addition, such disclosure of traffic data is incompatible with Article 6 of that directive.

Any violation of these rights and obligations is unacceptable unless it fulfils three fundamental criteria, in accordance with Article 8 (2) of the European Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950, and the European Court of Human Rights' interpretation of this provision: a legal basis, the need for the measure in a democratic society and conformity with one of the legitimate aims listed in the Convention The legal basis must precisely define the limits and the means of applying the measure: the purposes for which the data may be processed, the length of time they may be kept (if at all) and access to them must be strictly limited. Large-scale exploratory or general surveillance must be forbidden[9]. It follows that public authorities may be granted access to traffic data only on a case-by-case basis and never proactively and as a general rule.

These criteria coincide with the above mentioned provisions in Article 13 of Directive 95/46/EC and Article 14 of Directive 97/66/EC.

---

[7] Available at: see footnote 1.

[8] Law enforcement authorities require also access to real-time connection information, data concerning active connections (so-called "future traffic data").

[9] See especially the Klass judgment of 6 September 1978, Series A No 28, pp.23 et seq., and the Malone judgement of 2 August 1984, Series A No 82, pp. 30 *et seq*. The Klass judgement, like the Leander judgement of 25 February 1987, insists on the need for "effective guarantees against abuse" "in view of the risk that a system of secret surveillance for the protection of national security poses of undermining or even destroying democracy on the ground of defending it". (Leander judgement, Series A No 116, pp. 14 et seq.). The Court notes in the Klass judgement (paragraphs 50 *et seq.*) that assessing the existence of adequate and effective guarantees against abuse depends on all the circumstances of the case. In the particular case, it considers that the surveillance measures provided for in German legislation do not permit exploratory or general surveillance and do not contravene Article 8 of the European Convention for the Protection of Human Rights. German legislation provides the following guarantees: surveillance is confined to cases in which there are indications for suspecting a person of planning, committing or having committed certain serious criminal acts; measures may be ordered only if the establishment of the facts by another method is without prospects of success or considerably more difficult; and even then, the surveillance may cover only the specific suspect or his presumed "contact-persons".

Divergence of national rules[10]

Concerning the period during which traffic data may be stored, Directive 97/66/EC only allows preservation for billing[11] purposes and only up to the end of the period during which the bill may lawfully be challenged. This period however varies significantly in Member States. In Germany for example, telecommunications operators and telecommunications services providers are allowed to store the data necessary for billing up to 80 days for the purpose of proving the correctness of the billing[12]. In France, it depends on the status of the operator: the "traditional" telecommunications operator is allowed to keep traffic data up to one year on the basis of the law fixing the period during which the bill can be challenged. This period is fixed to 10 years for other operators. In Austria, the telecommunications law does not fix a concrete period up to which traffic data may be stored for billing purposes, but limits it to the period during which the bill can be challenged or during which the payment can be claimed. In the United Kingdom, according to the law, the bill can be challenged during 6 years, but operators and service providers store the relevant data for about 18 month. In Belgium for example, the law does not define such a period, but the biggest telecommunication service provider has fixed this period to 3 month in its general conditions. Another practice can be observed in Portugal where, since the period is not fixed by law, the national data protection supervisory authority decides on a case by case basis. It is interesting to note that in Norway the period is fixed to 14 days.

The current practice of ISPs is also not homogenous: it seems that small ISPs preserve traffic data for very short periods (a few hours) because of lack of storage capacity. Bigger ISPs who are able to afford such storage capacity may be preserving traffic data for up to a few months (but this may depend on their billing policies: per connection time or per fixed period).

For the purpose of law enforcement, the Dutch telecommunications law obliges telecommunications operators and service providers to collect and store traffic data for three month.

Obstacles for the functioning of the Internal Market

This divergence raises potential obstacles within the Internal Market for the cross-border provision of telecommunications and Internet services but as well effective law enforcement may be hampered by such divergent periods. It could be invoked that an ISP established in one Member State is not entitled to store traffic data longer than fixed in the Member State where the customer is living and using its service. Or an ISP may be pressed to keep traffic data longer than allowed in its own Member State because the laws of the country of the users require so. In case of billing for roaming in mobile telephony it is not the foreign operator who recovers the bill, but the national operator of the subscribers concerned. Different periods for storing data necessary for the billing may thus lead to the same problems as described for ISPs. The rule of the applicable law set out in Article 4 of Directive 95/46/EC does solve this problem only to the extent that the ISP is the controller and established only in one Member State, but not in cases where he is established in several Member States with different periods or where he processes traffic data on behalf of the controller.

10. The Commission is currently in the process of analysing the laws of those Member States who have notified national measures implementing Directive 97/66/EC and Directive 95/46/EC. See implementation table concerning Directive 95/46/EC available at: see footnote 4.
11. And, where necessary, for interconnection payments between telecommunications operators, see Article 6 paragraph 2 of Directive 97/66/EC.
12. If the bill is challenged during this period, the relevant data can of course be kept until the dispute is settled.

Recommendation

In view of the above, the Working Party considers that the most effective means to reduce unacceptable risks to privacy while recognising the needs for effective law enforcement is that traffic data should in principle not be kept only for law enforcement purposes and that national laws should not oblige telecommunications operators, telecommunications service and Internet Service providers to keep traffic data for a period of time longer than necessary for billing purposes.

The Working Party recommends that the European Commission proposes appropriate measures to further harmonise the period for which telecommunication operators, telecommunications service and Internet Service providers are allowed to keep traffic data for billing and interconnection payments[13]. The Working Party considers that this period should be as long as necessary to allow consumers to be able to challenge the billing, but as short as possible in order not to overburden operators and service providers and to respect the proportionality and specificity principles as being part of the right to privacy. This period should be aligned on the highest standard of protection observed in Member States. The group draws attention to the fact, that in several Member States periods of no longer than 3 months have been successfully applied.

The Working Party furthermore recommends that national governments take into account these considerations.

Done at Brussels, 7 September 1999

For the Working Party

The Chairman

Peter HUSTINX

13. In view of this objective, there is no justification for the operating distinctions relating to privateor public operators.

Appendix 5

ARTICLE 29 DATA PROTECTION WORKING PARTY RECOMMENDATION 4/99

ON THE INCLUSION OF THE FUNDAMENTAL RIGHT TO DATA PROTECTION IN THE EUROPEAN CATALOGUE OF FUNDAMENTAL RIGHTS

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

Having regard to Articles 29 and 30(3) of that Directive,

Having regard to its Rules of Procedure, and in particular Articles 12 and 14 thereof,

HAS ADOPTED THE FOLLOWING RECOMMENDATION:

At its meeting on 4 June in Cologne, the European Council decided to draw up a charter of fundamental rights of the European Union. In its decision, the Council noted that "there appears to be a need, at the present stage of the Union's development, to establish a charter of fundamental rights in order to make their overriding importance and relevance more visible to the Union's citizens."

The Working Party, composed of those responsible for data protection in the Member States of the European Union, wholeheartedly supports the European Council's initiative to draw up an EU charter of fundamental rights. It notes that some European countries have incorporated fundamental rights on data protection into their constitution. In others, these rights have acquired constitutional force through case law.

In their decisions and judgments, the European Commission and the European Court of Human Rights have developed and defined a fundamental right based on various human rights which relate to the protection of personal data.

Finally, under the new Article 286 of the Treaty on European Union, Community acts on data protection have applied to the European institutions and bodies since 1 January 1999.

Inclusion of data protection among the fundamental rights of Europe would make such protection a legal requirement throughout the Union and reflect its increasing importance in the information society.

The Working Party therefore recommends that the European Commission, the European Parliament and the Council of the European Union include the fundamental right to data protection in the charter of fundamental rights. The Working Party is prepared to help in the drawing-up of the charter.

Done at Brussels, 7 September 1999

For the Working Party

The Chairman

Peter HUSTINX

Appendix 6

REGISTRATIONS 1996 – 1999

	1996	1997	1998	1999
Data controllers by economic sector				
Civil Service Departments/Offices	99	97	100	106
Local Authorities and Vocational Education Committees	118	118	114	112
Health Boards and public hospitals/clinics	41	42	40	40
Third level education	31	32	33	35
Primary and secondary schools	14	18	19	22
Commercial state-sponsored bodies	75	74	70	72
Non-commercial and regulatory public bodies	93	116	129	139
Associated banks	22	22	25	35
Non-associated banks	47	52	54	51
Building societies	8	8	8	7
Insurance and related services	120	134	137	149
Credit Unions and Friendly Societies	439	451	457	448
Credit reference/Debt collection	19	20	22	23
Direct marketing	42	45	50	54
Miscellaneous commercial	12	19	34	36
Private hospitals & clinics/other health	81	88	92	103
Doctors, dentists & other health professionals	242	269	306	369
Pharmacists	495	515	511	501
Political parties & public representatives	31	84	78	95
Religious, voluntary & cultural organisations	31	40	42	53
Subtotal	***2,060***	***2,244***	***2,321***	***2,450***
Data Processors	***293***	***327***	***329***	***325***
Total	**2,353**	**2,571**	**2,650**	**2,775**

[1]A data processor is defined in ***section 1(1)*** of the Act as "*a person who processes personal data on behalf of a data controller*". ***Section 16(1)(d)*** requires data processors "*whose business consists wholly or partly in processing personal data on behalf of data controllers*" to register.

Appendix 7

REPORT OF THE COMPTROLLER AND AUDITOR GENERAL

In accordance with Paragraph 9 of the Second Schedule to the Data Protection Act, 1988, I have audited the Account on pages 58 and 59 which is in the form approved by the Minister for Justice, Equality and Law Reform.

I have obtained all the information and explanations that I have required.

As the result of my audit it is my opinion that proper accounting records have been kept by the Department of Justice, Equality and Law Reform on behalf of the Data Protection Commissioner and the Account, which is in agreement with them, properly reflects the transactions of the Commissioner for the year ended 31st December, 1999.

Joseph J. Meade

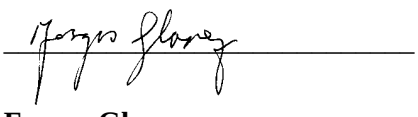
For and on behalf of the Comptroller and Auditor General

21 July 2000

ACCOUNT OF RECEIPTS AND PAYMENTS IN THE YEAR ENDED 31 DECEMBER, 1999

1998		1999
£	Receipts	£
309,451	Moneys provided by the Oireachtas (note 1)	342,251
220,778	Fees	233,674
530,229		575,925
	Payments	
213,498	Salaries & Allowances (note 2)	226,352
8,012	Travel & Subsistence	8,904
20,274	Office & Computer Equipment	27,095
831	Furniture & Fittings	2,873
4,628	Equipment Maintenance & Office Supplies	11,369
4,614	Accommodation Costs (note 3)	23,767
13,148	Communication Costs	12,407
5,128	Incidental & Miscellaneous	4,688
38,328	Education & Awareness	22,408
990	Legal & Professional Fees	2,388
309,451		342,251
220,778	Payment of fee receipts to Vote for the Office of the Minister for Justice, Equality and Law Reform	233,674
530,229		575,925

The statement of accounting policies and principles and notes 1 to 3 form part of these accounts.

Signed  Date 21 July 2000

Fergus Glavey
Data Protection Commissioner

ACCOUNT OF THE OFFICE OF THE DATA PROTECTION COMMISSIONER

STATEMENT OF ACCOUNTING POLICIES AND PRINCIPLES

1. GENERAL

The Office of the Data Protection Commissioner was established under the Data Protection Act, 1988. The Commissioner's functions include supervising the implementation of the Act, ensuring compliance with its provisions, investigating complaints, dealing with contraventions of the Act, encouraging the preparation of codes of practice, establishing and maintaining a Register of data controllers and data processors who are required to register, and rendering mutual assistance to other data protection authorities.

2. ACCOUNTING ARRANGEMENTS

2.1 Moneys provided by the Oireachtas
The Commissioner does not operate an independent accounting function. All expenses of the Office are met from subhead F of the Vote for the Office of the Minister for Justice, Equality and Law Reform. The expenditure figures in these accounts detail the payments made by the Department of Justice, Equality and Law Reform on behalf of the Office.

2.2 Fees
Fees paid to the Data Protection Commissioner in respect of registration and enquiries are transferred intact to the Vote for the Office of the Minister for Justice, Equality and Law Reform as appropriations-in-aid.

NOTES TO THE ACCOUNT

1. Moneys provided by the Oireachtas
Vote 19 — Office of the Minister for Justice, Equality and Law Reform Subhead F £342,251.

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

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

3. Premises
The Commissioner occupies premises at the Irish Life Centre, Talbot Street, Dublin 1, which are provided by the Office of Public Works, without charge. The provisional cost to the Office of Public Works of the accommodation provided in 1999 was £50,274 (1998 cost £54,720). In addition, a sum of £19,055 was recouped to the Office of Public Works for other accomodation costs for 1999 and prior years.

NOTES