Submission by the Business Law and Technology Committees to the Minister for Justice, Equality and Law Reform on The Data Protection (Amendment) Bill 2002

For further information please contact:

Sylvia McNeece

The Secretary

Business Law Committee

The Law Society of Ireland

Blackhall Place

Dublin 7

Telephone: 01 6724946

Fax: 01 6724803

E-Mail: s.mcneece@lawsociety.ie

CONTENTS:

KEY RECOMMENDATIONS:

- **Ireland needs to build upon the success of the *Electronic Commerce Act, 2000* and focus on how the protection of the right to privacy in an electronic environment can confer a lasting competitive advantage on Ireland. (P.10 – P.12)**
- **The Irish law should be consolidated into a single Statute, which would clearly state the rights and duties of Irish data subjects and controllers. This Act should facilitate and not impede the development of Ireland's information society and economy. (P.10 – P.12)**
- **The role of the Data Protection Commissioner should be evaluated, reforms should be implemented to ensure that the Data Protection Commissioner's office has the power, expertise and financial resources to provide statements of practice, recommendations and opinions setting out how Data Protection Law applies to certain sectors. (P.35 – P.43)**
- **Key terms such as consent should be clearly defined in the Irish legislation. (P.19 – P.23)**
- **A review should be undertaken so that rights, duties, and exemptions under the Act should be clearly defined to take account of the role played in Irish society of certain institutions, professions and technologies including An Garda Siochana, professional advisors such as accountants or solicitors and technologies such as CCTV. (P.30 – P.35 and P.45)**
- **The Data Protection Commissioner should be able to issue statements of practice on his own initiative; (P.43)**
- **The institutional structures of the Data Protection Commissioner should be examined, in particular, a review should be undertaken of the feasibility and suitability of establishing a Data Protection Board as a part of the Irish Data Protection Authority. This Board could have functions such as hearing appeals from decisions of the Data Protection Commissioner or the approval of Statements of Practice; (P.40 – P.41)**
- **Data Protection needs to be made more coherent in accordance with the State's commitment towards better regulation. In particular a review should be undertaken of the division of responsibility for Data Protection within the State, at present this is divided between several different departments, notably the Department of Communications, the Marine and Natural Resources and the Department of Justice, Equality and Law Reform.**

PART I - THE FRAMEWORK FOR DATA PROTECTION.

- **A review should be undertaken of the protection given to all forms of data whether personal or confidential;**
- **A review should be undertaken of the extent to which Ireland should introduce an exemption from Data Protection law for "activities of the State in areas of criminal law;**
- **A review should be undertaken of whether or not it is appropriate or possible to avail of any further exemption in respect of the economic well-being of the State when the processing operation relates to State security matters.**
- **The Bill should specify exactly what duty of care a Data Controller owes a data subject for the purposes of section 7 of the Data Protection Act, 1988.**
- **The Bill should make it clear that if the Data Protection Commissioner does not object to registration, then once a purpose is registered the Data Controller may regard that purpose as being "legitimate" and it may fully process data in accordance with that purpose for the purposes of the law of torts.**
- **There should be a clear requirement that the purpose of processing be disclosed to the data subject at the time of collection, and no consent can be valid unless the purpose of processing is first disclosed to the data subject.**
- **A review of the suitability of introducing a principle of data economy, similar to that provided for in Germany should be undertaken.**
- **The data subject's consent should be defined in the text of the Bill;**
- **A review should be undertaken of the following issues:**
    - **Should consent be 'informed', that is must the data subject be given information about how his data is to be processed before he gives his consent?**
    - **Should the definition of consent define the categories of information to be given to the data subject before he gives his consent?**
    - **Should the consent be in writing (as in Germany)?**
    - **Should it be possible to revoke consent (as in Greece)?**
    - **Should some element of the definition of consent in the Directive concerning the processing of personal data and the protection of privacy in the telecommunications sector be included?**
- **An analysis to be undertaken of how the requirement that data cannot be retained "…for longer than is necessary…" must interact with other legislation and the possible inclusion of an exemption in the 2002 Bill such as a provision that data may be retained for whatever period is required by the other legislation or a State Agency for the purposes of gathering tax or preventing fraud.**

- **A provision to be included allowing for the archiving of material, whereby it could be retained for the purposes of record keeping but would not be available for processing in the day-to-day business of a firm and access to it would be restricted.**
- **An analysis to be undertaken of the consequences of establishing 'data banks' or archives which would store personal data on behalf of third parties.**
- **An examination of the interaction of the Data Protection (Amendment) Bill, 2002 and the Equal Status Act, 1998 should be undertaken.**
- **An evaluation of the Report of the Lindsay Tribunal should be carried out, and proper provisions for the control and monitoring of Health information should be installed. The provisions of the 2002 Bill should be reviewed in this context to ensure that Data Protection laws facilitate the treatment of disease and do not impede it.**
- **Section 20 should either exempt all data in manual files until 24th October 2007 or apply in full from the date of enactment.**

PART II - THE RIGHTS OF THE DATA SUBJECT.

- **A review should be undertaken of whether it is necessary to amend section 5 of the 1988 Act so as to extend the exemptions therein to agencies such as the Office of Director of Corporate Enforcement.**
- **A review should be undertaken of how the Data Protection Act will integrate with the provisions of the Sex Offenders Act 2001.**
- **A review should be undertaken of how the 2002 Bill will impact upon the role traditionally played in Irish Society by professional advisors such as solicitors in particular by the giving of legal assistance as well as advice.**
- **A review should be undertaken of whether it would be possible to avoid the implications of section 4(13) as inserted by section 5 of the 2002 Bill by requiring potential employees to make Freedom of Information Act Requests.**
- **The 2002 Bill should more clearly define the terms used in relation to the right to object or alternatively, the Data Protection Commissioner should have the power to issue recommendations or opinions that would clearly set out the terms under which Data subjects could successfully object to the processing of their data.**
- **It should be made easier to seek definitive guidance from the Courts as to what specific terms actually mean.**
- **The Data Protection Commissioner should issue a recommendation, statement of practice or opinion setting out how the rules on Automated processing of Data are to be followed.**

- **A review should be undertaken of whether or not the exemption for expressions of opinion given by Prison Governors in section 4A of the 1988 Act as inserted by section 5 of the 2002 Bill should be extended to other persons such as the Director of Corporate Enforcement.**

PART III - THE SUPERVISION OF DATA PROTECTION:

- **An analysis to be undertaken of how the Data Protection Commissioner's duties will expand under the new legislation, and a review of how the Data Protection Commissioner's office can be adequately resourced and staffed should be considered.**
- **The setting up of an expert advisory Board to advise the Data Protection Commissioner to be considered.**
- **A review should be undertaken of whether or not the functions of the Data Protection Commissioner and the Information Commissioner should be merged into a single office.**
- **The Data Protection Commissioner should have the clear power to issue recommendations, or opinions on best practice in a particular area. The Data Protection statements of practice Commissioner should have the power to do so on his own initiative without receiving a complaint and without necessarily forming an opinion that a contravention of the Act is occurring.**
- **An examination might be undertaken of whether an internal means of appeal should be provided by the Data Protection Commissioner's Office and, if so, how that internal appeal might be provided.**
- **Where a dispute arose between the Data Protection Commissioner and a third party as to the interpretation of a statutory term or the application of one of the terms of a European Directive, a straightforward means of appealing the dispute to the High or Circuit Courts should be provided.**
- **The Data Protection Commissioner should not have to bear the burden of interpreting the meaning of different terms in the Data Protection Act. If a particular term should prove controversial then the Data Protection Commissioner should be able to refer the interpretation of that term to the Circuit court using a procedure that will be cheap, quick and easy to use.**
- **The Data Protection Commissioner should have the power to enter into "co-operation agreements" similar to those that the Competition Authority is required to enter into.**

PART IV - DATA PROTECTION IN THE INFORMATION SOCEITY:

- **The 2002 Bill fails to take advantage of such exemptions as are provided by recital 17 of the Directive, in relation to CCTV systems. A review should be undertaken of whether or not it is**

appropriate for Ireland to take advantage of those exemptions and how those exemptions could be implemented into Irish law.

- **The 2002 Bill should clearly define which types of CCTV system are covered by the Data Protection Act, in particular it should define whether or not analogue or digital systems are covered and whether or not a CCTV system has to be connected to a recorder to be covered.**
- **An examination should be undertaken of the suitability or necessity of including some form of warning in public areas to inform Data subjects that they are subject to surveillance.**
- **A specific offence of identity theft should be introduced.**
- **Ireland needs to develop a coherent strategy on unsolicited direct mail. Analysis should be undertaken as to how the Bill will interact with the implementation of the Directive on certain legal aspects of information society services and the Directive on privacy and electronic communications and the Directive on distance selling of financial services.**
- **The amended section 2(7) of the 1988 Act to be inserted by section 3 of the 2002 Bill needs to be amended to reflect modern realities that data may be collected as well as kept for the purposes of direct marketing.**
- **The Act should make it clear that where data is gathered for the purposes of direct marketing then a data subject should be clearly informed that they have a right to object to such marketing.**
- **If it is decided to introduce "opt-in/opt-out" registers under other legislation for e-commerce or electronic communications then these should be extended to all forms of direct marketing.**
- **A review should be undertaken of how Data Protection law interacts with the operation of the Irish domain name system.**
- **A review should be undertaken of how the Data Protection Bill 2002 will impact upon the use of Electronic signatures and Advanced Electronic Signatures under the Electronic Commerce Act 2000.**
- **Clearer provisions on how credit reference agencies are to be regulated should be introduced, whether as a part of the Act, an SI or detailed recommendations from the Data Protection Commissioner**
- **Irish recommendations or guidelines on the Data Protection policies to be followed in employment should be issued as a matter of some urgency.**
- **A review should be undertaken of how Data Protection law will impact upon competition in different sectors of the economy and what provisions might be introduced to facilitate competition.**

PART V - JURISDICTION.

- **A review should be undertaken on how Ireland may adapt the provisions of section 10 of the 2002 Bill to take account of the role that non-EU multinationals play in the Irish economy.**

PART VI - ENFORCEMENT.

- **Consideration should be given to the use of Data Protection audits by licensed Data Protection auditors and some statutory exemption from liability for any Data Controller which is so audited;**
- **The appointment of Data Protection officers within firms should also be analysed;**
- **The criminal provisions of the 1988 Act should be integrated with the implementation of the cybercrime convention.**

AFTERWORD:

- **More should be done to make Irish people aware of the threats posed to their privacy, such educational work should be targeted at specific groups, individuals should be made aware of how their privacy can be invaded on-line, while companies should be made aware that failure to abide by Data Protection law may expose them to tort liabilities.**
- **A review should be undertaken of how Ireland can publicise the existence of data processing operations in accordance with Article 21 of the Directive.**

INTRODUCTION:

Information and communications technologies have conferred huge benefits on Ireland in the past decade, and Ireland will rely on these industries for economic and employment growth in the next. If Ireland makes the correct choices it can develop an information society and economy that thrives as a sector in the Information society that Europe is seeking to build. Some of these choices will have to be made in the field of privacy. Privacy is a basic human right, it is a right recognised by both the Irish Constitution and the European Convention on Human Rights[1]. Modern information and communications technologies allow the monitoring of human behaviour in a variety of ways that effectively infringe upon the right to privacy. Carrying a mobile phone means that one's location is being constantly monitored, reading newspapers on-line means that one's interests can be followed and ordering from an on-line supermarket leaves one's diet open to examination. In modern Ireland the best way to preserve one's privacy is to avoid modern technologies. However, if improving technology is seen as requiring low or no privacy, Ireland is in danger of creating an important incentive for opting out of the Information society that Ireland hopes to build.

Data Protection law offers a solution to this problem. By laying down strict rules for how personal data is processed it enables companies, businesses and the State to process this data while preserving the privacy of the individual. Data Protection law should be a facilitator, giving individuals the assurances which enable them to engage in the information society while setting out clear rules that enable businesses to process data without infringing upon the privacy of their customers or employees. Unfortunately, poor implementation can mean that Data Protection laws restrain rather than facilitate. Poorly drafted Data Protection laws can limit innovation, restrict the development of new products and deny both consumers and businesses the benefits of information and communications technologies. The object of Data Protection is not to limit the introduction of new technologies, rather it is to ensure that new technologies do not infringe upon privacy. A primary aim of any Data Protection law must be to adapt to new technologies and products and Ireland has an excellent opportunity to do this in the *Data Protection (Amendment) Bill, 2002.* Ironically, this opportunity stems from Ireland's failure to implement the Data Protection Directive 95/46 in time. Ireland has delayed so long that it can now implement both this Directive and the Directive on Privacy and Electronic Communications [2] at the same time. This gives Ireland the opportunity to create a Data Protection framework that is specifically adapted to the Internet, this framework would be unique in Europe and could have the effect of conferring significant competitive advantage upon Ireland.

[1] Article 8.
[2] Directive 2002/58/Ec of The European Parliament and of the Council Of 12 July 2002 concerning the processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive On Privacy and Electronic Communications)

Europe's Data protection laws are unique, and they are very much a product of Europe's history. The Data Protection Act, 1988 implemented the Strasbourg Convention of 1981, this viewed data processing as something carried on a centralized mainframe bought from IBM or Digital. Centralisation meant that data processing could be easily controlled and monitored, the Convention and the 1988 Act anticipated that processing might well be sub-contracted to a "data-processor". The Convention did not anticipate the explosion in computer use that followed the launch of the PC. The 1995 Directive was drafted in the wake of the fall of the Berlin Wall, East Germany was revealed as a State that maintained a centralized bureaucracy that held extensive details about its citizens and the citizens of other states such as West Germany. The 1995 Directive did not anticipate growth in Internet use and how new activities such "internet cookies" and identity theft would all become serious threats to the privacy of Europe's citizens.

There is a strong argument to be made that the technological concepts upon which the 1995 Directive is based are now obsolete. The centralized and controlled monitoring of an individual's data does not pose the greatest threat to an individual's data privacy, rather it is the carrying on of a host of different minor monitoring activities that are truly invasive. Arguably privacy is not threatened by a single, centralized Big Brother, rather it is threatened by a host of 'little brothers'. Web-sites that use 'cookies' to monitor what pages a person reads, mobile phones which monitor an individual's location and directory sites which set out the contents of electoral registers all pose a considerable threat to privacy. Anyone who wishes to search such distributed stores of personal data will be able to gather considerable data about an individual's lifestyle and habits on-line without ever becoming known to the data subject or anyone else.

Many of the greatest threats to privacy arise in the context of telecommunications and Internet use. An unfortunate feature of EU legislation is that, instead of amending the 1995 Directive to take account of the particular circumstances of the telecommunications sector, an entirely new Directive to deal with privacy on telecommunications networks was devised. The Internet rendered this Directive obsolete almost immediately, so a new Directive on Privacy and Electronic Communications has recently become law. This split means that, while the implementation of Data Protection law in general is a function of the Department of Justice, Equality and Law Reform the implementation of Data Protection law for the Internet and telecommunications systems is a function of the Department of Communications, the Marine and Natural Resources. So the Data Protection Commissioner and the ODTR, shortly to become the Commission for Communications Regulation, must interact in some way. The Department of Enterprise, Trade and Employment also has responsibilities in this area, as it is in the process of implementing the Electronic Commerce Directive that will deal with spamming and direct marketing.

This split in legislative and regulatory function disregards the realities of Data Protection: an individual's privacy is constantly under threat in many different fields. The Data Protection Commissioner is highly effective in protecting the privacy of citizens when they interact with established institutions such as banks,

insurance companies or credit bureaux. However, the structures of Data Protection, in Ireland and Europe, were not designed to deal with distributed threats to privacy as are now emerging on-line.

Information technology has become pervasive throughout society, this gives a single individual the power to collect, process and exploit vast amounts of personal data. Pervasive use of information technology means that most businesses cannot function without processing personal data as a matter of course. Data Controllers are no longer just large businesses with in-house lawyers and IT Departments, they now include small shopkeepers, single practitioner solicitors' practices and home office workers. Ireland has to review how it implements Data Protection law to facilitate these new types of Data Controller. Data Protection law is complex, but a failure to comply with it carries serious penalties and these penalties could have a serious economic impact. Section 7 of the 1988 Act makes it clear that data subjects can sue for damages where their Data Protection rights have been breached, although it is difficult to assess at what level the courts would assess damages in a Data Protection case. However, given that appeals from decisions of the Data Protection Commissioner must be taken to the Circuit court, this Court would seem the logical place in which to issue proceedings in respect of a breach of Data Protection law. The Circuit Court jurisdiction is currently between €6,346.72 and €38,092.14 although this is due to rise to between €20,000 and €100,000[3] with the implementation of the Courts and Court Officers Act, 2002. Automated processing of data may mean that large numbers of data subjects will have their personal data processed in an identical manner. So any breach of Data Protection law may give rise to a very large number of plaintiffs with identical claims and entitled to identical awards for damages. A bank which interfered with the Data Protection rights of 20,000 of its customers might face a total claims worth between €126 and €761 million at the current level of the Circuit Court jurisdiction, if such actions were brought under the raised jurisdiction the bank might face claims of between €400 million and €2 billion. This means that Ireland has to implement its Data Protection laws in a clear manner that can be easily followed by both businesses and consumers. A key recommendation in this regard is that all the relevant legislation, the 1988 Act, the Data Protection Directive and the Directive on Privacy and Electronic Communications should be implemented as a single item of consolidated legislation. This would create a clear framework for the public to follow, the alternative is to have businesses and consumers leafing through two or more Irish statutes, two or more European Directives and an assortment of Statutory Instruments. The latter approach will inevitably lead to confusion and increase the cost of complying with Data Protection Law.

Key Recommendations made in this submission are:

- **Ireland needs to build upon the success of the *Electronic Commerce Act, 2000* and focus on how the protection of the right to privacy in an electronic environment can confer a lasting competitive advantage on Ireland.**

[3] Sections 13 & 14 of Courts and Court officers Act 2002.

- **The Irish law should be consolidated into a single Statute, which would clearly state the rights and duties of Irish data subjects and controllers. This act should facilitate and not impede the development of Ireland's information society and economy.**
- **The role of the Data Protection Commissioner should be evaluated, reforms should be implemented to ensure that the Data Protection Commissioner's office has the power, expertise and financial expertise to provide recommendations and opinions setting out how Data Protection law applies to certain sectors.**
- **Compliance with Data Protection law needs to be made easier in other ways, so that businesses and other Data Controllers can manage the liabilities that may be imposed by Data Protection law.**

PART I - THE FRAMEWORK FOR DATA PROTECTION.

The 2002 Bill sets out a number of rules that must be complied with if Data Protection is to be both lawful and legitimate.

The scope of Data Protection.

In general the laws of the Member States protect the privacy of living people, Ireland's 1988 Act is typical in this regard, it provides that personal data is "…data relating to a living individual…"[4]. Italy however takes a different approach and it provides that:

> "This Act …shall further ensure the protection of the rights of legal persons and of any other body or association."

Many different types of information will be valuable in an Information society, not just those relating to individuals. Arguably the failure to give clear legal protection to all forms of information places Ireland at a competitive disadvantage in contrast with other European nations. Rights in Confidential Information are recognized by the courts, however, the failure to legislate for them may discriminate against the owners of these rights. The creation of an offence of theft of information was advocated by the Law Reform Commission and there is already such an offence in the USA, France and Germany.

The Directive makes it clear that it only applies to limited areas of activity, Article 3 of the Directive states:

> "This Directive shall not apply to…processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,"

Given the costs involved in complying with Data Protection law, one of the main challenges for the State is to ensure that it benefits from these exemptions to the maximum extent. The scope of the Directive is quite well defined. The only area where some element of interpretation does arise is in relation to recital 13: "the processing of personal data that is necessary to safeguard the economic well-being of the State does not fall within the scope of this Directive where such processing relates to State security matters". Ireland has a limited the scope of the exemptions under the 1988 Act to:

- Personal data that in the opinion of the Minister (for Justice) or the Minister for Defence are, or at any time were, kept for the purpose of safeguarding the security of the State;

- Personal data consisting of information that the person keeping the data is required by law to make available to the public.

The above exemptions are far narrower than those permitted under the 1995 Directive. By not availing of the exemption for the criminal justice system or public security, the State may be exposing itself to serious liabilities. A good example is the Sex Offenders Act 2001, this requires sex offenders to notify the Gardai of his or her name and address and date of birth. This means that the Gardai will be Data Controllers in respect of this data, which seriously limits how the Gardai can process this material. The Gardai would have to first analyse whether or not they were in compliance with the 1988 Act before this data was accessed in an investigation. So if the Gardai were to access a list of sex offenders as a part of a criminal investigation, this access would be limited to what was relevant to that investigation and when the investigation was concluded all material relating to that access would have to be destroyed. The Gardai have spent a lot of money introducing information technology systems, it is likely that these systems are designed and used to process large amounts of personal data. As noted above a failure to comply with the 1988 Act may prove very costly, and this may impose considerable liabilities on the Minister for Justice and the Gardai in future. A review needs to be undertaken, of the extent to which Ireland should introduce an exemption from Data Protection law for "activities of the state in areas of criminal law". There are strong arguments to be made that Data Protection law is particularly important in criminal law cases and that the State should have to abide by the same rules that it is imposing upon citizens.

As regards the Member States, Belgium has an interesting provision in relation to sex offenders, article 6(3) of the Belgian Act provides that:

> "…the processing of personal data relating to sexual life is permitted if the processing is carried out by an association…or institution of which the main objective is the evaluation, support and treatment of persons of whom the sexual conduct may be qualified as a criminal offence…"

Denmark provides that data relating to "criminal records, serious social problems and other purely private data" can be processed by the Criminal Courts and Police[5]. It also provides that: "This Act shall not apply to the processing of data which is performed on behalf of the intelligence services of the police and the national defence"[6]

[4] 1988 Act, Section 2
[5] Danish Act, article 2(4)

Recommendation:

- **A review should be undertaken of all forms of information that may need to be protected by the law.**
- **A review should be undertaken of the extent to which Ireland should introduce an exemption from Data Protection law for "activities of the State in areas of criminal law";**
- **A review should be undertaken of whether or not it is appropriate or possible to avail of any further exemption in respect of the economic well-being of the State when the processing operation relates to State security matters.**

"Fairly and Lawfully"

Section 2(1)(a) of the Act, as will be substituted by section 3 of the 2002 Bill provides that:

> "data shall have been obtained, and the data shall be processed, fairly and lawfully".

This is basically identical to the Directive, and some other Member states take a similar approach such as Italy[7], Portugal[8], Austria[9] and Belgium[10]. One example is Holland, which provides:

> "Personal data shall be processed in accordance with the law and in a proper and careful manner"[11]

The Danish Act requires that "Data shall be processed in accordance with good practices for the processing of data[12]". If Ireland were to implement a similar provision, it would presumably mean that somebody would have to set out what those 'good practices' were. Such a process would interact well with the proposal that the Data Protection Commissioner should issue practice recommendations[13]. The Finnish Act develops this theme further, it provides:

> "The controller shall process personal data lawfully and carefully, in compliance with good processing practice, and also otherwise so that the protection of the data subject's private life and the other basic rights which safeguard his/her right to privacy are not restricted without a basis

---

[6] Danish Act, Article 2(11).
[7] Italy, Article 9(1)(a)
[8] Portugal, Article 5(1)(a)
[9] Austria, Section 6(1)(1)
[10] Belgium, Article 4(1)(1)
[11] Holland, Article 6.
[12] Denmark, Act on Processing of Data, section 5(1).
[13] See recommendation – below.

provided by an Act. Anyone operating on the behalf of the controller, in the form of an independent trade or business, is subject to the same duty of care[14]"

This includes the requirement that the Data Controller follow good practice, but it goes further by setting out the duty of care that the Data Controller owes the data subject. Setting out a duty of care in this way would be quite significant for the Irish legislation as section 7 of the 1988 Act states that the Data Controller owes the data subject a duty of care but does not specify what that duty actually is.

Recommendation

- **The Bill should specify exactly what duty of care a Data Controller owes a data subject for the purposes of section 7 of the Data Protection Act 1988.**

The Purpose of Processing:

Data can only be obtained for one or more specified, explicit and legitimate purpose, it may not be further processed in a manner incompatible with that purpose or those purposes and it must be adequate, relevant and not excessive in relation to the purpose or purposes for which the data was obtained or processed. Deciding upon the definition of "purpose" is one of the key decisions for any person or company that intends to engage in data processing. The Data Controller cannot simply ignore the definition of his purpose, as he will have to define it at several stages:

1. The Bill requires virtually all Data Controllers to register (with a few limited exceptions). The information which must be supplied by the Data Controller in its application for registration are specified by the Data Protection Commissioner himself, but section 19(2) of the 1988 Act is clear, it provides that:

   > "A Data Controller…shall not: keep or use personal data for a purpose other than the purpose or purposes described in the entry".

   This makes the definition of purpose essential, if a Data Controller defines its purpose too narrowly it will be seriously limited in how it processes data. On the other hand the Data Controller cannot define purpose too broadly, as the Data Protection Commissioner may refuse to permit the processing[15].

[14] Finland, Personal Data Act (523/1999) section 5.
[15] 2002 Bill, section 11, inserting new section 12A into 1988 Act.

2. Data cannot be processed fairly for the purposes of section 2(1)(a) of the 1988 Act unless the Data Controller has informed the data subject of the "purpose or purposes for which the data are intended to be processed". Once data is obtained from the data subject then the Data Controller will be bound by the purposes which were disclosed to the data subject at the time of collection.

Given the importance of the definition of purpose it would seem appropriate that the purpose of the gathering of data should be clearly disclosed to the Data subject at the time of collection. Again this is related to the definition of consent, if consent is to be valid it should be informed.

Recommendation:

- **The Bill should make it clear that if the Data Protection Commissioner does not object to registration, then once a purpose is registered the Data Controller may regard that purpose as being "legitimate" and it may fully process data in accordance with that purpose for the purposes of the law of torts.**
- **There should be a clear requirement that the purpose of processing be disclosed to the data subject at the time of collection, and no consent can be valid unless the purpose of processing is first disclosed to the data subject.**

Adequate Relevant and not excessive:

Data can only be processed where the processing is "adequate, relevant and not excessive in relation to the purpose for which they were collected". Again this highlights the importance of the definition of processing discussed above. The German Act[16] takes perhaps the broadest approach to Data Protection, it provides in relation to "data avoidance and data economy" that:

> "The organisation and choice of data-processing systems shall be guided by the objective of collecting, processing and using as little personal data as possible. In particular, use shall be made of the possibilities of anonymisation and pseudonymisation where possible and where the effort entailed is proportionate to the interests sought to be protected."

Recommendation:

[16] Until 1989, East Germans were subject to extraordinary levels of monitoring by State Security Services such as the notorious Stasi.

- **A review of the suitability of introducing a principle of data economy, similar to that provided for in Germany, should be undertaken.**

Consent:

The Irish Act does not define what it means by the consent of the data subject. Consent is important for two aspects of the Bill: firstly it provides that: "Personal data shall not be processed…unless…the data subject has given his or her explicit consent…"[17]; a similar provision applies in respect of sensitive data[18]. The Bill does not offer any clear definition of what "explicit consent" may actually mean, and confusion may be caused by section 6B of the Act[19], which provides that the data subject must give his "consent" without any qualification. The Bill does not explain how this differs from "explicit consent", if at all. It does state that "a word or expression that is used in this Act and also in the Directive has, unless the context otherwise requires, the same meaning in this Act as it does in the Directive[20]". The Directive provides three meanings for the term consent, it states that:

1. "the data subject's consent" shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed"[21].
2. It states that the consent of the Data subject must be given "unambiguously"[22];
3. It states that the consent of the Data subject must be "explicit".[23]

The Directive does not give any guidance on how these different definitions of consent are to be reconciled. It is understandable that the framers of the Bill would not want to take on this burden themselves, however, its clarity would be greatly improved if a definition of consent was included directly in its text, rather than expecting users to read the Act in conjunction with the Directive. The definition of consent is highly significant, personal data and sensitive data can only be processed if the consent is received (unless the Data Controller brings himself within one of the other exceptions). There are a number of requirements, if consent is to be valid under the Directive:

[17] 2002 Bill, section 4, inserting new section 2A(1) into 1988 Act.
[18] 2002 Bill, section 4 … see also 2002 Bill section 7 inserting new section 6A(3)(a) into the 1988 Act which refers to explicit consent.
[19] 2002 Bill section 7, inserting a new section 6B into the 1988 Act.
[20] 2002 bill section 2, inserting new section 3A into the 1988 Act.
[21] Direction 95/ Article 2(h)
[22] Directive , article 7
[23] Directive, article 8.

1. It must be "freely given"; so a consent cannot be forced out of an individual, no consequences can flow from a refusal to give a consent;
2. It must be "specific"; a generalized consent ("I agree to let Z Data Controller do whatever he wants with my data") would not be valid; the requirement of specification is reinforced a number of times.
3. It must be "informed"; the Data subject must be told how his data will be processed. This is significant, as the Data subject must be given certain information under the Bill[24], it appears from the Directive that this information should be disclosed to the Data subject before his consent is given.
4. There must be an "indication of his wishes by which the Data subject signifies his agreement…"; it is for the Data subject to indicate how his data is to be processed. Again this forces any consent to be highly specific.
5. Specification is also reinforced by the requirement that it be "explicit" or "unambiguous".

What would a definition of consent look like?

Not every EU Member State includes a definition of consent, for example, the UK does not do so. Definitions of consent can also vary considerably between Member States, with some including more detail than others, Finland describes consent as:

> "…any voluntary, detailed and conscious expression of will, whereby the data subject approves the processing of his/her personal data".

Similarly Denmark defines consent as:

> "'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed;"

The Directive does provide that certain information must be given to the data subject[25]. Where the different Member States vary is that not all of them have an explicit requirement that this information be given prior to the giving of consent. Ireland will not explicitly require that the data subject be given information before his consent is given, the Bill requires that:

[24] 2002 Bill, section 4, inserting new section 2D into 1988 Act.
[25] Directive Articles 10 and 11

> "…the Data Controller ensures, so far as practicable, that the data subject has, is provided with, or has made readily available to him or her, at least the information…[26]".

This is less than a requirement that the data subject be informed of anything, information should be available to the data subject but only "as far as is practicable". There is no explicit requirement as to when this information must be available, but the 2002 Bill does provide that the following information must be provided to the data subject:

(a) "the identity of the Data Controller,
(b) if he or she has nominated a representative for the purposes of this Act, the identity of the representative,
(c) the purpose or purposes for which the data are intended to be processed, and any other information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data to be fair to the data subject such as information as to the recipients or categories of recipients of the data, as to whether replies to questions asked for the purpose of the collection of the data are obligatory, as to the possible consequences of failure to give such replies and as to the existence of the right of access to and the right to rectify the data concerning him or her".

Somewhat more limited information has to be supplied in situations where the information is not obtained directly from the data subject. One of the main challenges in drafting a definition of consent is how to integrate the definition of consent with the requirement to supply information and in particular when this information must be supplied. Austria defines consent as:

> *"* the valid declaration of intention of the data subject, given without constraint, that he agrees to the use of data relating to him in a given case, after having been informed about the prevalent circumstances;"

The German definition is perhaps the most extensive:

> "Consent shall be effective only if it is based on a free decision of the data subject. The data subject shall be advised of the intended purpose of collection, processing or use and, where the particular circumstances so require or at his request, of the consequences of refusing consent. Consent shall be given in writing except where special circumstances render some other form appropriate. If consent is to be given in writing simultaneously with other declarations, special prominence shall be given to the declaration of consent"

[26] 2002 Bill section 4, inserting new section 2D into 1988 Act.

However, Greece arguably goes further:

> "The data subject's Consent" shall mean any freely given, explicit and specific indication of will, whereby the data subject expressly and fully cognisant signifies his informed agreement to personal data relating to him being processed. Such information shall include at least information as to the purpose of processing, the data or data categories being processed, the recipient or categories of recipients of personal data as well as the name, trade name and the address of the Controller and his representative, if any. Such consent may be revoked at any time without retroactive effect."

The Greek provision that consent can be revoked must interact with the right of the data subject to object to processing, but the right to object in the Directive is limited, as it must be on "compelling legitimate grounds" and it must be "justified"[27]. No such limitations appear in the Greek definition of consent. Similarly the Danish Act provides that: "The data subject may withdraw his consent"[28]. Although the Spanish Act does provide that consent can be withdrawn but only if it is justified, it provides that: "The consent…may be revoked when there are justified grounds for doing so and the revocation does not have retroactive effect".

Perhaps the most relevant definition of consent is that given in the Directive on Privacy and Electronic Communications. This defines consent as:

> "Consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an Internet website[29].

Some element of this definition might be included in the 2002 Bill as it makes it clear that ticking a box on a website is sufficient.

Recommendation:

- **The data subject's consent be defined in the text of the Bill;**
- **A review be undertaken of the following issues:**
    - **Should Consent be 'informed', that is must the Data subject be given information about how his Data is to be processed before he gives his consent?**

[27] Directive, article 14.
[28] Denmark, section 38.

- **Should the definition of consent define the categories of information to be given to the Data subject before he gives his consent?**
- **Should the Consent be in writing (as in Germany)?**
- **Should it be possible to revoke consent (as in Greece)?**
- **Should some element of the definition of consent in the Directive on Privacy and Electronic Communications be included?**

How long should data be retained?

The 2002 Bill imposes limitations on the length of time for which data can be retained, it provides that data:

> "…shall not be kept for longer than is necessary for that purpose…"

The purpose referred to is the "specified, explicit and legitimate purpose" for which the data was obtained, this purpose would be set out in the registration of the Data Controller. The 2002 Bill does not specify precisely how long data should be kept for, although other Member States do limit the amount of time for which some forms of data can be held. Denmark provides that information relating for creditworthiness cannot be retained for longer than 5 years[30], similarly Spain provides that credit data can only go back 6 years. One concern is that Irish law sets up a conflict, since there is other legislation that may require the retention of data for very long periods of time indeed. The Dublin Solicitors Bar Association would point out that the Law Society encourages its members to keep records for at least 12 years[31].

The Revenue Commissioners:

The Revenue Commissioners for example will typically expect that data be retained for 6 years or more, although many taxpayers may prefer to retain records even longer. This obviously is not a problem when records relating to the individual taxpayer are being retained, but records will relate to other data subjects. Customer receipts and details may contain detailed personal information, as will employee pay slips. The Taxes Consolidation Act 1997 does place taxpayers under an obligation to keep certain records in section 886(2)(a), which provides that:

> "Every person who—

---

[29] Recital 17, Directive on privacy and electronic communications.
[30] Denmark, 20(3)
[31] The Business Law and Technology Committees would like to thank the Dublin Solicitors Bar Association for reviewing this submission.

(i) on that person's own behalf or on behalf of any other person, carries on or exercises any trade, profession or other activity the profits or gains of which are chargeable under Schedule D,
(ii) is chargeable to tax under Schedule D or F in respect of any other source of income, or
(iii) is chargeable to capital gains tax in respect of chargeable gains,
shall keep, or cause to be kept on that person's behalf, such records as will enable true returns to be made for the purposes of income tax, corporation tax and capital gains tax of such profits or gains or chargeable gains".

These records must be kept in written form for six or more years[32], there are a wide variety of similar provisions relating to the retention of records for six or more years such as section 121(5)(e) and section 263(2)(a). Given the complexity of tax law and the consequences for failure to comply many taxpayers will regard 6 years as the minimum period for which records should be retained.

The Statute of Limitation Acts 1957 - 2000

This sets out strict time limits for the period during which an action may be taken, for example personal injury actions may only be taken within the three year period set out at section 11 of the 1957 Act. Actions for breach of contract and tort may be brought up to six years after the events giving rise to a cause of action. However, there are exceptions to this, in particular the Statute of Limitations (Amendment) Act, 1991 provides that actions for personal injuries can be taken outside this period in certain circumstances. The Committee of European Data Protection Commissioners set up by Article 29 of the Directive would suggest that annual assessments of employee performance should only be retained for two to three years. However, if an employee should be dismissed or disciplined as a result of consistently failing such assessments, then that employee will retain the right to sue for breach of his contract of employment for up to six years after the date upon which he was dismissed or disciplined.

Archiving Data:

The National Archives Act 1986 requires the preservation and retention of data held by the State. Section 7 of the Act states in relation to the Retention and disposal of Departmental records, that:

"…Departmental records shall…be retained and preserved in the Department of State in which they were made or are held, and shall not in any case be disposed of…".

There are exceptions to this rule, copies of records can be disposed of, records can be transferred to the National Archives or the Director of the National Archives can warrant the disposal of the records. Many

[32] Section 886(4)

of these records will contain personal data, their preservation means that they are being retained long after the purpose for which the data was originally collected has ended. Comprehensive State archives have an important function, some reconciliation of the National Archives Act, 1986 with the 1988 Act needs to be achieved. The Finnish Act has specific provisions relating to the archiving of data:

> "(1) Separate provisions apply to the use and protection of personal data files which have been transferred to the possession of the archive authorities, as well as to the disclosure of data from such files. However, when disclosing personal data from a private file, the archive authority shall take into account the provisions in this Act on the processing and disclosure of personal data, unless this, in view of the age or nature of the data recorded in the file, is manifestly unnecessary for the protection of the privacy of the data subjects.
>
> (2) A personal data file which is significant for purposes of scientific research or otherwise may be transferred for archiving to an institution of higher education or to a research institute or authority operating on a statutory basis, where the National Archives have granted a permission for such archiving. The National Archives may grant corporations, foundations and institutions a permission to archive personal data files compiled in their own activities and fulfilling the requirements above. In the permission the National Archives shall lay down rules for the protection of the files and for the monitoring of the use of the personal data.
>
> (3) Before granting a permission referred to in paragraph (2), the National Archives shall reserve the Data Protection Ombudsman an opportunity to issue an opinion on the matter[33]."

Archiving data offers a logical solution to the problem of preserving data for compliance with legislation after the original purpose for holding it has expired. Data banks or archives might be run by accredited third parties, under the supervision of the Data Protection Commissioner. These would store personal data on behalf of third parties and their relationship with those third parties would be governed by a contract. The third party would only be able to access the data in accordance with certain conditions such as: in response to a legitimate request from the Revenue Commissioners or other State Agency; in response to a request from the Data subject himself; in response to a Court Order for Discovery; or as a result of the initiation of a court action against the Data Controller. Some legislative provision for the creation of such archives might be considered.

Recommendations:

- **An analysis to be undertaken of how the requirement that data can not be retained "…for longer than is necessary…" must interact with other legislation and the possible inclusion of an exemption in the 2002 Bill such as a provision that data may be retained for whatever**

[33] Finland, section 35.

period is required by the other legislation or a State Agency for the purposes of gathering tax or preventing fraud.

- **A provision to be included allowing for the archiving of material, whereby it could be retained for the purposes of record keeping but would not be available for processing in the day-to-day business of a firm and access to it would be restricted.**
- **An analysis to be undertaken of the consequences of establishing 'data banks' or archives which would store personal data on behalf of third parties.**

Sensitive Data:

The processing of sensitive data gained a profile in Ireland when the payment of union subscriptions was used to identify striking teachers so that their wages could be stopped. The Directive provides that data such as this cannot be processed. One criticism of the Directive is that it appears to view the identification of a person's religious or political beliefs as something that is established off-line. The data subject will be asked what religion he is, or his political affiliation will be noted from his party subscription. The Directive could not have anticipated the situation where a person's political beliefs would be analysed from the books he orders from Amazon.com, or his religious beliefs discerned from his visits to Islamic web-sites. This could have serious implications for some Data Controllers such as employers. The 2002 Bill extends the limitation on what sensitive data can and cannot be processed. Section 2B as inserted by section 3 of the 2002 Bill, sets out 12 conditions under which sensitive data can be processed, such as where the data subject gives his explicit consent or it is necessary on health grounds. This implements Article 8 of the Directive. All Member States have similar provisions, but some go further than Ireland. One example is Belgium, which has a ban on the processing of health related data unless the processor can bring itself within one of 11 exceptions. Greece allows for the processing of sensitive data where the Data subject has given his consent, but it also provides:

> "The data subject has given his written consent, unless such consent has been extracted in a manner contrary to the law or *boons mores* or if law provides that any consent given may not lift the relevant prohibition."

Even more significantly, Greece will only permit the processing of sensitive data if the processor has a permit. This permit will only last a limited period of time and the complexities of applying for a permit should limit applications as the applicant must attend a hearing with the Greek Data Protection authority. The Spanish position is different as under its Constitution nobody can be obliged to state his or her ideology, religion or beliefs[34]. Although processing of sensitive data is permitted, subject to conditions, the Spanish Act does state that: "Files created for the sole purpose of storing personal data which reveal the

[34] Spain, Article 16(2) of the Spanish Constitution.

ideology, trade union membership, religion, beliefs, racial or ethnic origin or sex life remain prohibited". Denmark has specific provisions dealing with the processing of data relating to criminal convictions or serious social problems.

Although all the Member States must implement Article 8 of the Directive, many of them adapt the terms of the Directive to their own particular circumstances. Ireland might consider doing likewise. Ireland might consider how the terms of the *Data Protection (Amendment) Bill 2002* could be adapted to the circumstances of the *Equality Acts* or concerns about the processing of health data. The recent inquiry in relation to the Blood Transfusion Service has highlighted the importance of proper controls in relation to the processing and disclosure of health data. It would appear from the Report of the Lindsay Commission of Inquiry that a failure to propertly analyse and disclose health data may have had serious consequences for the health of many people.

Recommendation:

- **An examination of the interaction of the Data Protection Bill 2002 and Equality legislation should be undertaken.**
- **An evaluation of the Report of the Commission of Inquiry in the Hepatitis C scandal should be carried out, and proper provisions for the control and monitoring of Health information should be installed. The provisions of the 2002 Bill should be reviewed in this context to ensure that Data Protection laws facilitate the treatment of disease and do not impede it.**

Manual Files:

One of the most significant changes in the 2002 Bill is that it includes manual or paper files within the scope of Data Protection. Section 2 of the Bill provides that:

> "'manual data' means information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system;"

This does not mean that every piece of paper in an office will be subject to the law of Data Protection, only those items of paper that are held in a "relevant filing system", this is defined by section 1 as:

> "'relevant filing system' means any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to

individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible;"

So a filing cabinet or Rolodex that contained files sorted alphabetically by subject names would fall within this definition. This change in the law is being introduced pursuant to Article 3 of the Directive, so Ireland has no option but to implement it. However, given that information technology is now present in many Irish offices and companies, the impact of this provision may be limited. One issue that does arise is the transitional arrangements that will apply to manual data that already exists on the day when the 2002 Bill becomes law. Section 20 of the 2002 Bill states:

"(5) This Act, in so far as it— *(*a) amends section 2 of the Principal Act and applies it to manual data, and *(*b) inserts sections 2A and 2B into that Act, comes into operation on 24 October 2007 in respect of data held in manual filing systems on the passing of this Act.

(6) Notwithstanding *subsection (5*), a Data Controller shall, if so requested in writing by a data subject at any time after one month from the date of the passing of this Act but, in particular, when making a request under section 4 of the Principal Act—

(a) rectify, erase, block or destroy any data relating to him or her which are incomplete or inaccurate, or

(b) cease holding manual data relating to him or her in a way incompatible with the legitimate purposes pursued by the Data Controller."

The above means that Data Protection law will only fully apply from 24th October 2007 to data held in manual files that are in existence on the date that the Act becomes law. The Act will apply in full to data held in manual files from the date that the Act becomes law. It is doubtful that these transitional provisions offer any real comfort to the users of manual files. To take a hypothetical example: a filing system that contains 10,000 records on the date upon which the Bill becomes law will not be subject to the Act until 24th October 2007 in respect of the data that is in those files. However, if that filing system is being actively used then data will continue to be entered in those 10,000 records from the date upon which the Act becomes law and the Act will apply in respect of that data. So if data is entered in 2,000 files in the year following the Act becoming law, then the Act will apply to the data entered in those files since that date but not to the other 8,000 files. The problem for the Data Controller will be to identify the files in which data has been entered since the date of enactment and to then identify the data that has been entered in that file since that date. This is an impossible task, unless the Data Controller wishes to set up a separate filing system (which of course will be fully subject to the Act) to monitor changes in the original filing system. The only practical solution is to comply with Data Protection law in full in respect of all data held in the filing system. The only filing system which might benefit from this exemption is one in which data was no longer being entered, this might typically be an archive or a filing system that had fallen out of use.

Of course personal data should not be held if it is not being used as the holding of the data has no purpose, so it may be that the only filing systems which may benefit from this exemption are those that should be destroyed under the 1988 Act. Section 20 should either exempt all data in manual files until 24th October 2007 or apply in full from the date of enactment, the limited exemption currently provided is meaningless and will only cause confusion and expense.

Recommendation:

- **Section 20 should either exempt all data in manual files until 24th October 2007 or apply in full from the date of enactment.**

PART II - THE RIGHTS OF THE DATA SUBJECT.

The 2002 Bill amends the existing rights of the data subject such as the right to object and the right of access and creates new rights, such as the right to information and rights in the case of automated processing of data.

The Right of Access.

The Directive provides that exemptions may be provided to the right of access where it is necessary to safeguard:

> (a) national security;
> (b) defence;
> (c) public security;
> (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
> (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
> (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
> (g) the protection of the data subject or of the rights and freedoms of others.

Article 13 also creates an exemption in respect of data kept for personal or research purposes:

> "Subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual, Member States may, where there is clearly no risk of breaching the privacy of the data subject, restrict by a legislative measure (the right of access) when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics".

The above exemptions would appear to be consistent with the existing exemptions provided for in section 5(1) of the 1988 Act:

> "(a) kept for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders or assessing or collecting any tax, duty or other moneys owed or payable to

the State, a local authority or a health board, in any case in which the application of that section to the data would be likely to prejudice any of the matters aforesaid,

(b) to which, by virtue of paragraph (a) of this subsection, the said section 4 does not apply and which are kept for the purpose of discharging a function conferred by or under any enactment and consisting of information obtained for such a purpose from a person who had it in his possession for any of the purposes mentioned in paragraph (a) of this subsection,

(c) in any case in which the application of that section would be likely to prejudice the security of, or the maintenance of good order and discipline in—

(i) a prison,

(ii) a place of detention provided under section 2 of the Prison Act, 1970,

(iii) a military prison or detention barrack within the meaning of the Defence Act, 1954, or

(iv) Saint Patrick's Institution,

(d) kept for the purpose of performing such functions conferred by or under any enactment as may be specified by regulations made by the Minister, being functions that, in the opinion of the Minister, are designed to protect members of the public against financial loss occasioned by—

(i) dishonesty, incompetence or malpractice on the part of persons concerned in the provision of banking, insurance, investment or other financial services or in the management of companies or similar organisations, or

(ii) the conduct of persons who have at any time been adjudicated bankrupt, in any case in which the application of that section to the data would be likely to prejudice the proper performance of any of those functions,

(e) in respect of which the application of that section would be contrary to the interests of protecting the international relations of the State,

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

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

(h) kept only for the purpose of preparing statistics or carrying out research if the data are not used or disclosed (other than to a person to whom a disclosure of such data may be made in the circumstances specified in section 8 of this Act) for any other purpose and the resulting statistics or the results of the research are not made available in a form that identifies any of the data subjects, or

(i) that are back-up data".

Although Ireland's economy and society have undergone serious changes in the 14 years since the 1988 Act became law, the above exemptions will remain unchanged under the 2002 Bill. This may appear surprising given that since 1988 the number of regulatory agencies have increased dramatically, a good example is the Office of Director of Corporate Enforcement established by the Company Law Enforcement Act, 2001. It is not clear how an independent agency such as this will benefit from this exemption pursuant to section 5 of the 1988 Act. The Office of the Director was established by the Company Law Enforcement Act 2001, and he has extensive powers under this Act, particularly with regard to information. One example is section 29 of the Act, which provides that the Director can make directions requiring companies to produce books or documents. This is a function that falls within the exemption provided for in Article 13(f) of the Directive: - "a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c) (public security), (d) (the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions) or (e) an important economic or financial interest of a member state or of the European Union, including monetary, budgetary and taxation matters)". Many of the activities that will be investigated by the Director will be criminal acts whether under the Companies Acts themselves or other legislation such as the Criminal Justice (Theft and Fraud Offences) Act 2001. These would therefore fall within Article 13(d), as the State has an important economic and financial interest in ensuring compliance with the companies Acts, other functions of the Director would probably fall within Article 13(e)[35]. So pursuant to the Directive the Director could be exempted from Section 2D (Principles of Data Protection), Section (Information to be given to the data subject), Section 5 (the Right of Access) and Article 21 (publicising of Data Protection operations). However, the Act does not take advantage of these potential exemptions. Arguably, the Director could be entitled to rely upon the exemption from the Right of Access contained in section 5(1)(a) but only to a limited extent. This means that if the Director should collect information from a company, he will have to inform any person mentioned in that information pursuant to section 5 of the 2002 Bill. The Director will be limited in how he can deal with this information by the Data Protection Act 1988, so he will have to destroy it when his investigation of a particular company ends. Data subjects may object to the processing of data that relates to them, and will be able to seek access to the data held by the Director pursuant to section 4. Obviously, it would be very useful to any person facing a prosecution under the Companies Acts to know what documents the Director held that related to them. Complying with Data Protection Law will weaken the functioning of the Director of Corporate Enforcement, it will place him under an unnecessary administrative burden, distract him from his proper function and expose him to unnecessary liabilities. To the extent that the Director investigates criminal offences, as are many breaches of company law, he can be excluded from the scope of Data Protection law[36]. In other cases the Director should be able to avail of exemptions from many of the 1988 Act's more onerous provisions. Similar

[35] The functions of the Director are set out in full in Section 13 of the Company Law Enforcement Act 2001
[36] Article 3 of the Directive

arguments can be made with respect to many other regulatory agencies such as the Competition Authority, the ODTR or the Irish Aviation Authority. A review should be undertaken of whether it is appropriate or possible to exempt these agencies from all or some of the provisions of the 1988 Act.

The Right of Access and the Sex Offenders Act 2001.

Any school, health board or sporting association will be very anxious to ensure that it is not used by sex offenders to gain access to children. At present, organisations such as the ISPCC require potential employees to seek access to their records from the Gardai[37], but they will no longer be able to do this as a result of section 5 of the 2002 Bill which inserts new subsections in section 4 of the 1988 Act, subsection 4(13) provides that:

> "A person shall not, in connection with (i) the recruitment of another person as an employee, (ii) the continued employment of another person, or (iii) a contract for the provision of services to him or her by another person, require that other person
>
> (I) to make a request (for access) or
>
> (II) to supply him or her with data relating to that other person obtained as a result of such a request."

Once the above provision is enacted, the ISPCC would be committing an offence if it asked a potential employee to make an access request. It is an abuse of the Data Protection Act 1988 to require access requests be made in this way, but society regards child abuse as a more serious matter. Sex offenders must now comply with the terms of the Sex Offenders Act 2001, this makes it an offence for a sex offender to apply for a job that involves unsupervised access to a child or other vulnerable person without informing the employer that he or she is a sex offender. Employers cannot ask for this information, the onus is on the sex offender to supply it. The definition of sex offender is complex and it remains to be seen how the Act will work in practice. The Act also requires sex offenders to notify the Gardai with relevant information such as their name and address, it is unclear how these requirements will interact with the Data Protection Act, such as how long the Gardai can retain this information and the conditions under which Gardai involved in other criminal investigations can access information notified to the Gardai under the Sex Offenders Act 2001.

While it would be an offence for an employer to ask that a potential employee make an access request under the 2002 Bill, it would not be an offence to ask them to make a Freedom of Information request for records relating to them under the Freedom of Information Act 1997, (although this would not apply in the

[37] The Irish Times, 20th August 2002

case of criminal records as the Gardai are not subject to the Freedom of Information Act 1997). This may allow some employers to bypass the provisions of section 4(13) as inserted by section 5 of the 2002 Bill.

Privilege

Lawyers will receive considerable amounts of personal data from clients, in general this data will relate to the clients themselves, but it may also relate to third parties. If such third parties were to seek to enforce their right of access to personal data held by a solicitor a serious conflict of interest might arise for a solicitor. One example is the drafting of a will, this will usually be kept confidential until after the death of the testator. It is unclear from the legislation whether a third party would be able to seek to access a will prior to the death of a third party, by enforcing his or her right of access. When a client makes a will with a solicitor, they may supply their solicitor with ancillary information about those who benefit, or do not benefit under the will. This information will be retained by the solicitor in case the will is challenged after the death of the testator, again third parties may seek to access this information. Section 5(1)(g) provides that the right of access cannot be enforced in respect of data:

> "in respect of which a claim of privilege could be maintained in proceedings in a court in relation to communications between a client and his professional legal advisors or between those advisors"

Recent case law[38] may mean that the exemption provided above is insufficient to protect confidential information that could be provided by a testator to a solicitor when drafting a will. In particular legal professional privilege can only be invoked in respect of legal advice and not in respect of legal assistance. A review should be undertaken of how the 2002 Bill will impact upon the role traditionally played in Irish Society by professional advisors such as solicitors in particular by the giving of legal assistance as well as advice.

Recommendation:

- **A review should be undertaken of whether it is necessary to amend section 5 of the 1988 Act so as to extend the exemptions therein to agencies such as the Office of Director of Corporate Enforcement.**
- **A review should be undertaken of how the Data Protection Act will integrate with the provisions of the Sex Offenders Act 2001.**
- **A review should be undertaken of whether it would be possible to avoid the implications of section 4(13) as inserted by section 5 of the 2002 Bill by requiring potential employees to make Freedom of Information Act Requests.**

- **A review should be undertaken of how the 2002 Bill will impact upon the role traditionally played in Irish Society by professional advisors such as solicitors, in particular by the giving of legal assistance as well as advice.**

The Right to Information:

Issues relating to the right to information have been examined at p20 above in relation to the giving of consent.

The Right to Object:

Section 6A of the 1998 Act as amended by section 7 of the 2002 Bill gives a data subject the right to object to processing which is likely to cause substantial and unwarranted damage or distress to the data subject. Understanding of the terms "substantial" "unwarranted" "damage" and "distress" is crucial to any analysis of this section, but the Bill offers no definition. This is not unusual in Irish legislation where the interpretation of terms such as these is typically left to the courts. It may be very many years before the Irish courts ever offer an interpretation of these terms, however, Irish Data Controllers will have to start complying with these terms as soon as the Bill becomes law.

Recommendation:

- **The 2002 Bill should more clearly define the terms used in this section;**
- **Alternatively, the Data Protection Commissioner should have the power to issue recommendations or opinions that would clearly set out the terms under which Data subjects could successfully object to the processing of their data.**
- **It should be made easier to seek definitive guidance from the Courts as to what specific terms actually mean.**

New Rights under the 2002 Bill.

The 1995 Directive conferred new rights upon data subjects, in particular the right to object to processing likely to cause damage or distress and rights in relation to automated decision-making. The 2002 Bill changes the law on Data Protection by giving data subjects new rights such as the right to information and the right not to be subject to an automated decision. These new rights will change how Irish data subjects and controllers interact.

---

[38] *Miley –v- Flood,* 2001 1 ILRM 489.

Rights Related to Automated Decision Making:

Section 6B of the 1988 Act as it will be amended by section 7 of the 2002 Bill provides that a Data subject cannot be the subject of an automated decision which legally or significantly affects him or her. There is no definition of legal or significant effects but this would include decisions made in relation to performance at work, reliability or conduct.

Expressions of Opinion:

Data subjects are given the specific right to access statements of opinion about them under the Act. There are many areas where access to such opinions is clearly merited, for example in relation to applications for credit or references from employers.

> "a) Where personal data relating to a data subject consist of an expression of opinion about the data subject by another person, the data may be disclosed to the data subject without obtaining the consent of that person to the disclosure.
> b) Paragraph a) of this subsection does not apply to personal data held by or on behalf of the person in charge of an institution referred to in section 5(1)(c) of this Act and consisting of an expression of opinion by another person about the data subject if the data subject is being or was detained in such an institution.''[39],

One concern would be that this provision might interfere with the progress of criminal investigations, whether carried out by the Gardai or another agency such as the Director of Corporate Enforcement. A review should be taken of whether or not the exemption for expressions of opinion given by Prison Governors in section 4A of the 1988 Act as inserted by section 5 of the 2002 Bill should be extended to other persons such as the Director of Corporate Enforcement.

Recommendation:

- **The Data Protection Commissioner should issue a recommendation or opinion setting out how the rules on Automated processing of Data are to be followed.**

[39] Section 4A of the 1998 Act as inserted by section 5 of the 2002 Bill.

- **A review should be taken of whether or not the exemption for expressions of opinion given by Prison Governors in section 4A of the 1998 Act as inserted by section 5 of the 2002 Bill should be extended to other persons such as the Director of Corporate Enforcement.**

PART III - THE SUPERVISION OF DATA PROTECTION:

Ireland is now somewhat unusual in having a single Data Protection Commissioner, most other Member States instead have a number of Commissioners or a Data Protection Commission together with a Data Protection Council or Board. Given the expansion in the duties of the Data Protection Commissioner, it may be appropriate to broaden the range of expertise that is available to the Commissioner, such as by creating a Data Protection Board.

The Approach of other Member States.

Austria:

Austria has a Data Protection Commission *[Datenschutzkommissio*n] and a Data Protection Council *[Datenschutzra*t]. The Commission has six members, all of whom must have legal expertise and one of whom must be a judge. The appointment procedure is complex. The Council has a broad membership, including members of political parties and municipal councils. Its purpose includes debating issues of fundamental importance for Data Protection and commentating on legislation[40].

Belgium.

Belgium has a Commission for the Protection of Privacy, established at the Ministry of Justice. This has eight Members, one of whom must be a magistrate, who are appointed by the Belgian Parliament from lists submitted by the executive. The Chairman of the Commission has a full time post[41].

Denmark:

The Data Protection Agency consists of a council and a secretariat, the day-to-day business of the agency is carried out by the secretariat, which is headed by a Director. The Council is set up by the Minister of Justice, and is composed of a chairman, who is a legally qualified judge, and of six other members.

Finland.

Finland has a Data Protection Ombudsman and a Data Protection Board. The Data Protection Ombudsman provides direction and guidance on the processing of personal data, supervises the processing and makes

[40] Austria, Federal Act concerning the Protection of Personal Data (Datenschutzgesetz 2000 – DSG 2000) Part 7.
[41] Belgium, Law on Privacy Protection, Chapter VII.

decisions, as provided in this Act. The Data Protection Board deals with significant questions of principle relating to the processing of personal data[42].

Greece.

Greece has a Personal Data Protection Authority, which consists of a judge and six members. The Members must be University Professors or persons of high standing in the field of Data Protection. The President of the Authority is appointed on a full time basis.

The Kingdom of the Netherlands.

Holland has an Office of the Data Protection Commission, the Commission comprises a chairman and two members[43].

Italy.

The Italian Data Protection Authority is of interest as its members are elected directly by the Italian Parliament, the *Garante* consists of four members, two elected by the upper house and two by the lower. These members will then elect a chairman and he will have a casting vote in the event of a deadlock. The members must be persons ensuring independence and with proven experience in the field of law or computer science, and experts from both sectors have to be included.

Spain.

Spain has a Data Protection Agency, this consists of a Director of the Data Protection Agency assisted by a nine member Consultative Council. The Director must be appointed from among the Members of the Council.

United Kingdom.

The United Kingdom has integrated the role of Data Protection Commissioner with that of Information Commissioner for the processing of its Freedom of Information legislation. This has the effect of integrating different forms of expertise into the same office and prevents needless duplication.

[42] Finland, Personal Data Act (523/1999), section 38.
[43] Holland, Personal Data Protection Act , Chapter 9.

Should Ireland continue with a Single Commissioner?

The appointment of a single Commissioner is not unusual in Ireland, there is no question that the Data Protection Commissioner has performed very well in the exercise of his functions under the 1988 Act. However, the functions of the Commissioner will expand considerably under the new Bill and the Data Protection Commissioner will acquire new duties including the following:

- The carrying out of prior checking under the new section 12A;
- The refusal of applications for registration where there are no appropriate safeguards for the protection of privacy of sensitive data;
- The rules for the transfer of data outside the State are now more complex;
- The level of co-operation within Europe has increased as a result of the creation of the Working Party;
- The number of registrations will expand massively as a result of section 14 of the Bill.

It is important that the Commissioner has adequate and appropriate support in this difficult role. One option is to create a Data Protection Commission that has several members, an example of this is the creation of the Commission for Communications Regulation under the Communications Regulation Act 2002 in substitution for the Director of Telecommunications Regulation.

Should Ireland create a Board to assist the Commissioner?

The creation of such a Board was recommended for the Competition Authority by the Competition Law Review Group. This Board could have a valuable function, its expertise would be available to advise the Data Protection Commissioner; its members could substitute for him at European meetings; and its members could form panels of appeal from decisions of the Data Protection Commissioner; and it could approve statements of practice.

Should the office of the Data Protection Commissioner be amalgamated with other offices?

In the UK the Data Protection Commissioner and the Information Commissioner have been amalgamated into a single office. A similar change could be advocated here, the Information Commissioner does have to have regard to the laws of Data Protection, the Freedom of Information Act 1997 does have a function similar to the right of Access under the Data Protection Act 1988. An individual is able to access

information relating to them, held by the State[44] and amend those records if they are inaccurate[45]. Arguably this creates needless duplication and the two roles should be merged into a single office.

Recommendation.

- **An analysis to be undertaken of how the Data Protection Commissioner's duties will expand under the new legislation, and a review of how the Data Protection Commissioner's office can be adequately resourced and staffed should be considered.**
- **The setting up of an expert advisory Board to advise the Data Protection Commissioner to be considered.**
- **A review should be undertaken of whether or not the functions of the Data Protection Commissioner and the Information Commissioner should be merged into a single office.**

Should the Commissioner have the power to issue Statements of Practice?

The Data Protection Commissioner has the authority to approve codes of conduct under the 1988 Act and this authority is extended in the 2002 Bill. The Commissioner also has the power to issue regulations in relation to regulation. One power that the Data Protection Commissioner does not have is that of issuing general recommendations, such as the procedures to be followed by credit rating agencies or the protection of privacy in the workplace. The Data Protection Commissioner has adverted to issues such as these in his annual reports, and these comprise useful guides to what the Data Protection Commissioner considers appropriate. However, it should be possible for the Data Protection Commissioner to issue clear recommendations or statements of practice on pertinent topics. This would clarify the law for subjects and controllers and make compliance easier. At present, controllers and users who wish to discern the policies that the Data Protection Commissioner would like them to follow must read his Annual Report or find a relevant case study. Such recommendations would not necessarily be enforceable, but a Data Controller who followed their terms, would have a very good defence to any claim that its processing had infringed the rights of data subjects. This would be particularly important if a Data Controller was sued in tort, as a Controller could reasonably assume it was complying with Data Protection law if it followed the recommendations of the Data Protection Commissioner.

It has to be said that the Data Protection Commissioner is very open and available to discuss appropriate policies with interested parties and this informal approach worked very well under the 1988 Act. Given the considerable expansion in the number of controllers registering under the 2002 Bill, these increased

[44] Section 6, Freedom of Information Act 1997.
[45] Section 17, ibid.

workloads may render such informality impractical. Clear regulations would make both compliance and enforcement easier.

Co-ordination with other Agencies.

Data Protection issues will arise in a variety of different sectors, it is important that the Data Protection Commissioner should be able to co-ordinate his functions with that of other regulators. Some of the regulators with whom the Data Protection Commissioner may have to interact include:

- Information Commissioner
- Director of Consumer Affairs
- Competition Authority
- Equality Authority;
- Employment Appeals Tribunal;
- Sectoral Regulators, such as the Irish Aviation Authority and the ODTR.

Co-ordination between different regulators, agencies and authorities can become a serious problem, for example a conflict occurred between the ODTR and the Competition Authority in relation to the regulation of the Telecoms sector. The Competition Act 2002 dealt with this problem in section 34 which requires that:

> "There shall, as soon as practicable after the commencement of this section, be entered into between the (Competition) Authority and every one of the statutory bodies one or more agreements for the purposes of
> *(*a) facilitating co-operation between the Authority and the statutory bodies in the performance of their respective functions in so far as they relate to issues of competition between undertakings,
> *(*b) avoiding duplication of activities by the Authority and any of the statutory bodies, being activities involving the determination of the effects on competition of any act done, or proposed to be done, and
> *(*c) ensuring, as far as practicable, consistency between decisions made or other steps taken by the Authority and the statutory bodies in so far as any part of those decisions or steps consists of or relates to a determination of any issue of competition between undertakings, and each such agreement that is entered into is referred to in this section as a ''co-operation agreement''[46].

[46] Section 34(1), Competition Act 2001.

Given the growing importance of Data Protection issues in a wide variety of sectors it might be prudent to at least permit the drawing up of co-ordination agreements between the Data Protection Commissioner and other authorities.

Appeals.

At present appeals from decisions of the Data Protection Commissioner are to the Circuit Court. There have been very few of such appeals. The cost and complexity of court proceedings may discourage subjects and controllers from taking such appeals under the 1988 Act, however, the experience of regulators such as the ODTR suggests that court appeals may become an excessive burden on the time and resources of the Data Protection Commissioner. If it were decided to create a Data Protection Board, then one of its functions might be to hear appeals from decisions of the Data Protection Commissioner.

Appeals to the Circuit Court.

The law and the technology that applies to Data Protection are novel and complex. A procedure could be set in place by which a judge who wished to make him or herself available to deal with Data Protection matters could make this fact known to the President of the Circuit Court. That Judge would then be able to attend seminars on Data Protection law and have appropriate access to research and training facilities. This would enable the creation of a panel of judges who have expertise in Data Protection law.

Appeals on a Point of Law.

If an issue arose on a point of law such as how consent might apply in a given situation then it should be possible to provide for a limited form of appeal on a point of law only. This might involve the parties agreeing the facts of a given situation and agreeing the questions to be asked of the court. This would be similar to the case stated procedure already in use, a procedure that has been criticized as cumbersome. If such a procedure were to be put in place it would have to be cheap, quick and easy to use.

Recommendation:

- **The Data Protection Commissioner should to have the clear power to issue recommendations, statements of practice or opinions on best practice in a particular area. The Data Protection Commissioner should have the power to do so on his own initiative without receiving a complaint and without necessarily forming an opinion that a contravention of the Act is occurring.**

- **An examination might be undertaken of whether an internal means of appeal should be provided by the Data Protection Commissioner's office and, if so, how that internal appeal might be provided.**
- **Where a dispute arose between the Data Protection Commissioner and a third party as to the interpretation of a statutory term or the application of one of the terms of a European Directive, a straightforward means of appealing the dispute to the High or Circuit Courts should be provided.**
- **The Data Protection Commissioner should not have to bear the burden of interpreting the meaning of different terms in the Data Protection Act. If a particular term should prove controversial then the Data Protection Commissioner should be able to refer the interpretation of that term to the Circuit court using a procedure that will be cheap, quick and easy to use.**
- **The Data Protection Commissioner should have the power to enter into "co-operation agreements" similar to those that the Competition Authority is required to enter into.**

PART IV - DATA PROTECTION IN THE INFORMATION SOCIETY:

Data Protection law has to be applied to one of the swiftest developing industrial sectors, this forces the law to change as society and technology change also. New technologies ranging from CCTV cameras to Internet cookies may all impact upon the implementation of the Data Protection Directive in Ireland.

CCTV.

The use of Closed Circuit Television (CCTV) is now mundane in Ireland, CCTV cameras adorn petrol stations, banks, shops and buses. There are no estimates as to how many CCTV cameras currently exist in Ireland, but estimates in the UK run to well over one million. The Gardai currently supervise systems in Dublin City Center, Tralee and are installing one in Cork. It is planned to roll out ten more in the next year or two in town centres from Athlone to Bray. There is controversy about how effective CCTV actually is in deterring and detecting crime. A recent report from the National Association for the Care and Resettlement of Offenders (Nacro) in the UK suggested that cheaper methods, such as improving street lighting, can be far more effective[47]. Regardless of this debate, Irish people appear very happy to see the installation of this technology, which is changing and is moving away from the magnetic tape systems used in VCRs and instead digital recording and monitoring systems are being used. This makes it easier and cheaper to save recordings but, more significantly, such databases of video recordings are searchable. Face recognition software can trawl through such a database comparing faces in crowds with photographs of known criminals or others. This software achieved prominence last year when it was used at American Football's Super-bowl to identify 19 individuals with criminal records in a crowd of 100,000. Combining CCTV with face recognition software creates a very powerful tool for monitoring public-space, it could alert the Gardai as soon as a known criminal came into view. A system that automatically identifies and tracks individuals is far more invasive of privacy than one which remains passive until a human operator notices something suspicious. The London Borough of Newham in England has 300 CCTV cameras linked to a central database. It matches the faces it monitors with photographs of the faces of 100 known criminals, if it spots one it notifies the police who then commence surveillance of that individual. As a result crime rates have fallen by almost 35% since this system was introduced. The same system is used by South Wales Police to spot football hooligans, and an American chain, 'Borders' Bookshop recently announced that it was installing the same system used in Newham to identify shoplifters entering its UK stores.

The Gardai are bound by their own codes of practice in relation to the use of CCTV cameras. However, the 2002 Bill will apply to this technology. Recital 14 of the Directive states that:

[47] The Guardian, 29th June 2002.

> "…given the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, this Directive should be applicable to processing involving such data;"

So the Directive does apply to video and CCTV footage, however, it will only apply to the processing of data that is automated[48]. A further exemption is contained in recital 16 which provides that:

> "…the processing of sound and image data, such as in cases of video surveillance, does not come within the scope of this Directive if it is carried out for the purposes of public security, defence, national security or in the course of State activities relating to the area of criminal law or of other activities which do not come within the scope of Community law;"

So the systems operated by the Gardai could be outside the scope of the Directive, but systems aimed at preventing crime on private property, such as the typical CCTV system in a bank or petrol station is within the Directive. The Directive suggests that two types of issue might arise in relation to the use of CCTV cameras:

- What type of equipment is within the scope of the Bill? Is only digital and not analogue, or is analogue included if the system contains a search facility?
- What type of user is within the scope of the Bill, is it only the Garda systems that are exempt or is any system that is directed towards the identification of crime exempt? Is a CCTV system on a petrol station forecourt (private property) covered by the Directive, but is a system on a CIE bus, which is ultimately owned by the State covered?

The Bill does not mention the possibility that CCTV systems could be within the scope of the Directive at all. It does state that personal data means:

> '' 'data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the Data Controller;''[49],

This suggests that all forms of CCTV are covered by the Bill, since of course anybody can be identified from any videotape whether analogue or digital. Arguably, it covers any CCTV camera regardless of whether or not the camera is actually connected to a recorder. If the Bill were introduced in its current

[48] Recital 15.
[49] Section 1(a)(iii) of the 2002 Bill

form it would cause serious problems for many of the companies, local authorities and individuals who are using CCTV quite legitimately to protect their own property and persons. The provisions of other Member States vary, the Portuguese Act makes it clear that it applies to CCTV systems:

> "This Act shall apply to video surveillance and other forms of capture, processing and dissemination of sound and images allowing persons to be identified, provided the controller is domiciled or based in Portugal or makes use of a computer or data communication network access provider established on Portuguese territory."[50]

A primary concern with the failure to properly define the circumstances under which CCTV systems are within the ambit of the Directive means that Data subjects may not be aware of their rights and so may fail to enforce them. Similarly, Data Controllers who use CCTV systems may not be aware that they are subject to Data Protection law and so may unknowingly interfere with the rights of a data subject and face an action for damages in respect of that interference. Germany goes further than this, however, and it has specific provisions relating to "The surveillance of publicly accessible spaces using opto-electronic equipment":

> "(1) The surveillance of publicly accessible spaces using opto-electronic equipment
> (video surveillance) shall be lawful only if it is necessary
>
> 1. for public bodies to discharge their duties,
> 2. for exercising control over a premises or
> 3. to protect legitimate interests for specifically stated purposes and there are no grounds for believing that there are overriding legitimate interests of the data subjects at stake.
>
> (2) Notice of the fact that surveillance is taking place and the identity of the Data Controller shall be given by suitable means.
> (3) The processing or use of data collected in accordance with paragraph (1) shall be lawful if it is necessary for the attainment of the object pursued and if there are no grounds for believing that there are overriding legitimate interests of the data subjects at stake. The data may be processed or used for some other purpose only where necessary to counter threats to national and public security or for the investigation of crime.
> (4) If data collected by video surveillance are matched to a particular individual, the individual in question shall be notified of the processing or use in accordance with §§ 19a and 33.
> (5) The data shall be erased immediately when they are no longer necessary for the attainment of the purpose or where their further retention would be contrary to data subjects' legitimate interests."

[50] Portugal, Article 4(4)

The placing of prominent signs warning data subjects that they are subject to CCTV surveillance may be good practice for reasons other than Data Protection. Given that much of the reduction in crime rates associated with CCTV systems result from their deterrent effect, making CCTV systems more prominent will increase the deterrent.

Recommendation.

- **The 2002 Bill fails to take advantage of such exemptions as are provided by recital 17 of the Directive, in relation to CCTV systems. A review should be undertaken of whether or not it is appropriate for Ireland to take advantage of those exemptions and how those exemptions could be implemented into Irish law;**
- **The 2002 Bill should clearly define which types of CCTV system are covered by the Data Protection Act, in particular it should define whether or not analogue or digital systems are covered and whether or not a CCTV system has to be connected to a recorder to be covered.**
- **An examination should be undertaken of the suitability of including some form of warning in public areas to inform Data subjects that they are subject to surveillance.**

Identity Theft.

Identity fraud arises when someone takes over a totally fictitious name or adopts the name of another person with or without their consent[51]. Identity theft is an increasing problem, a report from the UK estimated that the minimum cost to the economy of identity fraud is £1.3 billion per annum. Some examples of the extent of identity fraud in 2000/01 are:

> • 3,231 driving tests were terminated prematurely because of doubts over the driver's identity;
> • 1,484 fraudulent passport applications were detected;
> • approximately 50 cases of fraudulent documentation were detected every month at Terminal 3, Heathrow Airport;
> • in the course of a two week exercise targeted at Portuguese documents in June 2001, 59 fraudulent documents were detected at selected UK ports and by the Benefits Agency National Identity Fraud Unit (NIFU). The majority were counterfeit identity cards, detected by the NIFU;
> • although there is little reliable information on the number of people trafficked into the UK, a recent Home Office study estimated that 1,500 women a year are trafficked for sexual exploitation;

[51] Home office Consultation paper "Entitlement Cards and identity Fraud", A consultation Paper, p39

• 564 cases involving identity fraud were identified by the Benefits Agency's Security Investigation Service, whose specialist teams investigate organised fraud cases across the country;
• in the private sector, the credit reference agency Experian estimated that around 1-2% of transaction value is lost through fraud and that about 3-5% of all fraud is identity fraud[52].

It is hard to imagine that Ireland would remain immune from such offences. The Internet makes offences of identity theft easier as it allows criminals to gather considerable information on-line about diverse individuals. Identity theft involves a number of actions that are particularly injurious to the Data Protection Rights of an individual such as the processing of sensitive data. However, a victim of identity theft is much more likely to be concerned that they have apparently acquired debts for things that they never bought. Identity theft is a crime facilitated by a failure to comply with Data Protection law rather than a breach of Data Protection law in itself. One solution to identity theft is to seriously limit the information that is available about individuals, however, ultimately this is impossible in an open information society. A better solution is to introduce an offence of identity theft in itself.

Recommendation:

- **A specific offence of identity theft should be introduced.**

Telecommunications & The Internet.

One of the main sectors upon which Data Protection law will impact is Telecommunications and the Internet. This reflects the reality that this is the sector where the privacy rights of the individual are most likely to be compromised. The EU has responded to concerns such as these by introducing a Directive 97/66/EC of the European Parliament and of the Council fo 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector automated storage and procesing of data relating to subscribers and users, this has now been replaced by a Directive on Privacy and Electronic Communications. Analysis of the implications of this new Directive for Data Protection in Ireland is outside the terms of this report, however it is important that there should be clear delineation of responsibilities for implementing the different items of legislation. The 1988 Act and 2002 Bill have to interact with telecommunications legislation, the Article 29 Committee is a good example of how this occurs as it issues recommendations in relation to Data Protection and Cybercrime; the open profiling standard; and on-line data collection. One example of how complex these problems can become is given by that of spamming and direct marketing.

[52] *ibid.*

Spamming & Direct Marketing.

Unsolicited e-mail or spamming is a considerable problem, one estimate from a study published by the EU suggests that the global costs of spamming may be as high as $10 billion a year[53]. The importance of this issue is reflected by the reality that it is dealt with by at least four different items of European legislation: the 1995 Directive itself; the Directive on electronic commerce; the Directive on privacy and electronic communications; and, the Directive on distance selling of financial services. This will inevitably lead to confusion and overlap between the legislative functions of different departments.

Both the 1988 Act and the 2002 Bill deal with direct marketing, an unusual feature of the amended section 2(7) is that like the 1988 Act it does not seem to anticipate a situation where data is collected for the purposes of direct marketing. This is anomalous in an age where data can be collected from any number of sources and in any number of ways. Some revision of section 2(7) should be undertaken to reflect modern realities. There is a need to explain how the amended section 2 will integrate with the requirement that the Data subject be given information about processing operations. In particular it needs to be made clear how the requirement that a data subject be told that he can object to processing in section 2(7) as amended by the 2002 Bill interacts with the provision in the new section 2D as inserted by section 3 of the 2002 Bill that the Data subject be given certain information. Other Member States are clearer on this point, Belgium requires that the Data subject be informed of his right to object to direct marketing as part of his right to information[54]

Neither the 2002 Bill nor the 1988 Act nor the 1995 nor 2002 Directives offer any specific definition of what "direct marketing" actually is, although the detail given by the 2002 Directive is reasonably clear.

> "1.The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.
> 2.Notwithstanding paragraph 1,where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use.

[53] Commission Of The European Communities, *Unsolicited Commercial Communications, Summary of Study Findings,* January 2001.
[54] Belgium, Article 9.1.c

> 3.Member States shall take appropriate measures to ensure that, free of charge, unsolicited communications for purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications, the choice between these options to be determined by national legislation.
>
> 4.In any event, the practice of sending electronic mail for purposes of direct marketing disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease, shall be prohibited.
>
> 5.Paragraphs 1 and 3 shall apply to subscribers who are natural persons. Member States shall also ensure, in the frame-work of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected[55]."

This does threaten to create anomalous situations, if Companies gather data in relation to direct marketing they will have to comply with the above, quite strict provisions, if they use that data for electronic marketing purposes. However, if they rely upon the existing postal system or other more traditional mechanisms they will not. One controversial solution to this problem is the use of opt-out registries, this would certainly be mandated by article 13(1) above, which states that spam can only be sent to those who have given their consent. The purpose of an opt-in registry is to list everyone who wishes to receive spam, the purpose of an opt-out registry is to list everyone who does not. An example of an opt-out registry is to be found in the Greek Act, which states:

> "Everyone shall be entitled to declare to the Authority that he does not wish data relating to him to be submitted to processing in order to promote the sale of goods or long distance services. The Authority shall keep a register for the identification of such persons. The Controllers of the relevant files must consult the said register prior to any processing and delete from their files the persons referred herein[56]."

The difficulty with such registries is that unscrupulous spammers can target them in search of e-mail addresses. It remains to be seen whether Ireland will require the creation of an opt-in or opt-out register as it implements the Directive on Electronic Commerce. If Ireland were to set up such a register under the E-commerce Directive, it would be logical to extend it to all forms of commerce.

Other countries limit the use of data for direct marketing in other ways. The Finnish Act provides that:

---

[55] Article 13
[56] Greece, article 13(3)

"(1) Unless such processing has been prohibited by the data subject, personal data may be collected and recorded, also for a reason not referred to in section 8(1), into a personal data file kept for the purposes of direct marketing, distance selling, other direct advertising, opinion polling and market research or for other comparable personalised mailing, if:

(1) the personal data file is used in a predetermined and short-term marketing campaign or other measure referred to in this paragraph and its contents do not compromise the protection of the privacy of the data subject; or

(2) the personal data file contains data solely on the name, title or occupation, age, sex and native language of the data subject as well as one distinguishing datum and the data subject's contact information;

(3) the file contains data pertaining to the duties or status of the data subject in business or public life, and it is used for the mailing of information relevant to the same.

(2) For a purpose referred to in paragraph (1), data referred in paragraph (1)(2) may be disclosed or used as sample criteria in a disclosure, unless the data subject has prohibited disclosure and if it is evident that the data subject is aware of such disclosure."

The above provision has the effect of seriously limiting the type of data which can be processed by direct mailers and does in fact eliminate much of the information that marketers would analyse to get a profile of an individual. This limitation would therefore limit the attractiveness of operating a direct mailing company in Finland.

Recommendation:

- **Ireland needs to develop a coherent strategy on unsolicited direct mail. Analysis should be undertaken as to how the Bill will interact with the implementation of the Directive on electronic commerce and the Directive on privacy and electronic communications and the Directive on distance selling of financial services.**
- **The amended section 2(7) of the 1988 Act to be inserted by section 3 of the 2002 Bill needs to be amended to reflect modern realities that data may be collected as well as kept for the purposes of direct marketing.**
- **The Act should make it clear that where data is gathered for the purposes of direct marketing then a data subject should be clearly informed that they have a right to object to such marketing.**
- **If it is decided to introduce "opt-in/opt-out" registers under other legislation for e-commerce or electronic communications then these should be extended to all forms of direct marketing.**

Domain Names.

The administration of the domain name system in Ireland involves the processing of some personal data, in particular in the provision of a "whois" directory that facilitates the identification of the owners of individual domain names.

Recommendation:

- **A review should be undertaken of how Data Protection law interacts with the operation of the Irish domain name system.**

Electronic Signatures.

The Irish system of regulating electronic signatures was widely recognized as innovative and pro-business when the *Electronic Commerce Act 2000* became law. One of the main functions of electronic signatures is to verify the identity of the signatory, this obviously has considerable implications for Data Protection. One example of a system of electronic authentication such as an electronic signature is the .net system offered by Microsoft. The Working Party set up under Article 29 of Directive 95/46 has undertaken an investigation of this technology and is considering the following issues in particular:

> "- The information given to the data subjects at the moment of collecting, further processing the data or transferring it to a third party, possibly located in a third country.
> - The value and quality of the consent given by the data subjects to these operations.
> - The Data Protection rules applied by the websites affiliated to .NET Passport.
> - The necessity and conditions of use of a unique identifier.
> - The proportionality and quality of the data collected and stored by .NET Passport and further transmitted to affiliated sites.
> - The exercise of the rights of the data subjects.
> - The security risks associated to these operations"[57]

Given the central role of the *Electronic Commerce Act 2000* in creating a perception abroad that Ireland is a center for e-commerce it is important that a review should be undertaken of how the *Electronic Commerce Act 2000* and the 2002 Bill will interact.

[57] EU Working Party on Data Protection, First orientations of the Article 29 Working Party concerning on-line authentication services, 11203/02/EN/final WP 60

Recommendation:

- **A review should be undertaken of how the Data Protection Bill 2002 will impact upon the use of Electronic signatures and Advanced Electronic Signatures under the Electronic Commerce Act 2000.**

Credit Rating Agencies.

The Data Protection Commissioner has identified the activities of credit rating agencies as being one of the areas where he consistently receives a large number of complaints, 19% of complaints received in 2001 related to credit reference agencies[58]. The regulation of credit rating agencies is a good example of an area where the Data Protection Commissioner might beneficially provide recommendations or opinions on his own initiative. The Report of the Data Protection Commissioner 2000 contains "Guidance Notes" for the Credit referencing sector[59] but the format of a report necessarily limits the detail which the Data Protection Commissioner can enter into, including such notes in an annual report makes it difficult to respond to issues immediately or to revise or refine those notes once made. Given the consistency with which issues relating to credit reference have been raised, it might seem appropriate to include more definite provisions in legislation as is done in Denmark. The Danish Act contains detailed provisions relating to the regulation of Credit Reference Agencies:

> **"19.** Any person who wishes to carry on business involving processing of data for assessment of financial standing and creditworthiness for the purpose of disclosure of such data (credit information agency) shall obtain authorisation to do so from the Data Protection Agency prior to commencing such processing, cf. section 50 (1) 3.
>
> **20.** – (1) Credit information agencies may only process data which by their nature are relevant for the assessment of financial standing and creditworthiness.
>
> (2) Data as mentioned in section 7 (1) and section 8 (4) may not be processed.
>
> (3) Data on facts speaking against creditworthiness and dating back more than 5 years may not be processed, except where it is obvious in any specific case that the facts in question are of decisive importance for the assessment of the financial standing and creditworthiness of the person concerned.

[58] Report of Data Protection Commissioner 2001, p11.
[59] Report of Data Protection Commissioner 2000, p36.

21. According to the provisions of section 28 (1) or section 29 (1), *(Information to be given to the Data subject)* credit information agencies shall notify the person to whom the data relate of the data mentioned in these provisions.

22. – (1) Credit information agencies shall, at any time, at the request of the data subject, notify him within 4 weeks, in an intelligible manner, of the contents of any data or assessments relating to him that the credit information agency has disclosed within the immediately preceding 6 months, and of any other data relating to the data subject that the agency records or stores at the time of the receipt of the request, whether in a processed form or by way of digital media, including any credit ratings.

(2) Where the agency is in possession of further material relating to the data subject, the existence and type of such further material shall at the same time be communicated to him, and he shall be informed of his right to inspect such material by personally contacting the agency.

(3) The agency shall further provide information on the categories of recipients of the data and any available information as to the source of the data referred to in subsections (1) and (2).

(4) The data subject may demand that the agency's communication as referred to in subsections (1) to (3) shall be given in writing. The Minister of Justice shall lay down rules on the payment of a fee for communications given in writing.

23. – (1) Data on financial standing and creditworthiness may be given only in writing, cf., however, section 22 (1) to (3). The agency may, however either orally or in a similar manner, disclose summary data to subscribers, provided that the name and address of the inquirer are recorded and stored for at least 6 months.

(2) Publications from credit information agencies may contain data in a summary form only and may be distributed only to persons or enterprises subscribing to notices from the agency. The publications may not indicate the civil registration numbers of data subjects.

(3) Disclosure of summary data on indebtedness may only take place where the data originate from the Danish Official Gazette, have been notified by a public authority under the rules laid down in Part 5 of this Act, or if the data relate to indebtedness in excess of DKK 1,000 to a single creditor and the creditor has obtained the written acknowledgement by the data subject of the debt being due and payable, or where legal proceedings have been instituted against the debtor concerned. Data on approved debt re-scheduling schemes may, however, not be disclosed. The rules referred to in the first and second clauses of this subsection shall also apply to the disclosure of summary data on indebtedness in connection with the preparation of broader credit ratings.

(4) Summary data on the indebtedness of individuals may be disclosed only in such a manner that the data cannot form the basis for assessment of the financial standing and creditworthiness of other persons than the individuals concerned.

24. Any personal data or credit ratings which turn out to be inaccurate or misleading shall be rectified or erased without delay.

25. Where any data or credit ratings which turn out to be inaccurate or misleading have already been disclosed, the agency shall immediately give written notification of the rectification to the data subject and to any third party who has received the data or the credit rating during the six months immediately preceding the date when the agency became aware of the matter. The data subject shall also be notified of any third party that has been notified under clause 1 of this section, and of the source of the personal data or credit rating.

26. – (1) Where a data subject requests the erasure, rectification or blocking of data or credit assessments which are alleged to be inaccurate or misleading, or requests the erasure of personal data which may not be processed, cf. section 37 (1), the agency shall reply in writing without delay and within 4 weeks from receipt of such a request.

(2) Where the agency refuses to carry out the requested erasure, rectification or blocking, the data subject may within 4 weeks from receipt of the reply of the agency or from expiration of the time-limit for replying laid down in subsection (1) bring the matter before the Data Protection Agency, which shall decide whether erasure, rectification or blocking shall take place. The provisions laid down in section 25 shall be correspondingly applicable.

(3) The reply of the agency in the cases mentioned in subsection (2) shall contain information about the right to bring the matter before the Data Protection Agency and about the time-limit for such submission.

Denmark is not the only country that has rules in relation to Credit Rating Agencies included in its Act. Finland also has lengthy provisions on this point:

"Section 20 — *Processing of personal credit data*

(1) A person engaged in credit data activity may record into a credit data file the name and contact information on a person, as well as data on a default in payment or performance, where:

(1) the default has been established by a judgment or judgment by default handed down by a court and no longer subject to appeal, by a measure undertaken by the enforcement authorities or by the protest of a registered bill of exchange; or the default has led to the official declaration of the insolvency of the data subject in enforcement proceedings;

(2) the default has led to the filing of a bankruptcy petition;

(3) the default has been acknowledged in writing by the data subject to the creditor; or

(4) the default relates to a hire-purchase scheme and under the Hire-Purchase Act (91/1988) entitles the seller to repossess the object, or relates to another consumer credit agreement and under the Consumer Protection Act (38/1978) entitles the creditor to terminate the agreement.

(2) The data referred to above in paragraph (1)(4) may be recorded only if there is a clause in the consumer credit agreement stating the situations in which the default in payment or performance can be recorded into the credit data file. Further prerequisites are that the creditor has at least 21 days earlier sent the debtor a written reminder which mentions the possibility of recording default data into the credit data file and that the debtor has been in default for at least 60 days from the original due date, mentioned in the reminder.

(3) In addition, data may be recorded in a credit data file on the entries contained in the debt adjustment register referred to in section 87 of the Act on the Adjustment of the Debts of a Private Individual (57/1993), on the placement of a person under guardianship and on the appointment of a trustee to administer the financial affairs of a person, and, on the request of the data subject, on the payment of the debt referred to in paragraph (1) and on a credit stoppage, where supplied by the data subject himself/herself.

(4) Personal credit data may be disclosed only to a controller engaged in credit data activity and to a person needing the data for purposes of granting credit or credit monitoring, or for another comparable purpose.

Section 21 — *Erasure of data in a credit data file*

The data referred to in section 20(1)(1)—(4) shall be erased from the credit data register as follows:

(1) the data referred to in subparagraph (1) after the lapse of four years from the establishment of the default;

(2) the data referred to in subparagraph (2) after the lapse of five years from the filing of the bankruptcy application;

(3) the data referred to in subparagraph (3) at the latest after the lapse of two years from the acknowledgement of the default; and

(4) the data referred to in subparagraph (4) at the latest after the lapse of two years from the recording of the entry on default."

Recommendation:

- **Clearer provisions on how credit reference agencies are to be regulated should be introduced, whether as a part of the Act, an SI or detailed recommendations from the Data Protection Commissioner**

Employment.

One of the most controversial areas of Data Protection is that of employment. The 2002 Bill does contain a number of provisions relating to employment such as the processing of sensitive data[60]; the issue of references[61]; or the prohibition on employers making access requests[62]. The Data Protection Commissioner made reference to work place Data Protection issues in his 1999 report[63] and the Article 29 Working Party of EU Data Protection Commissioners has issued a number of recommendations on such issues. Detailed guidelines should be given as to how the Data Protection Directive should be applied in the workplace as a matter of urgency. Failure to do so means that employees are unaware of their rights, while employers may be exposed to significant liabilities as they remain unaware of how they should implement Data Protection in this area. This failure to provide detailed guidance places Ireland at a competitive disadvantage vis-à-vis the UK that already has such guidelines. A particular concern is that in the absence of Irish guidelines, companies here may be tempted to follow the UK rules but this may expose Irish companies to risks as Irish and UK rules may differ.

Recommendation:

- **Irish recommendations or guidelines on the Data Protection policies to be followed in employment should be issued as a matter of some urgency.**

Competition.

Restrictions on access to personal data can pose a considerable difficulty for the development of competition in sectors such as public utilities. Sectors such as electricity and gas supply are characterized by a large incumbent operator, an incumbent must have access to a database of its own customers if it is to function effectively. However, if potential competitors cannot access the same information a significant barrier to competition may be created. This issue was dealt with in the Telecoms sector by giving the ODTR responsibility for managing the phone directory, a review should be undertaken of how Data Protection law will impact upon such sectors and what provisions might be introduced to facilitate competition.

[60] Section 2B as inserted by section 3 of 2002 bill.
[61] Section 4(4A) as inserted by section 5 of 2002 Bill.
[62] Section 4(13) as inserted by section 5 of 2002 Bill.
[63] Report of Data Protection Commissioner, 1999, p31

Recommendation:

- **A review should be undertaken of how Data Protection law will impact upon competition in different sectors of the economy and what provisions might be introduced to facilitate competition.**

PART V - JURISDICTION.

The 2002 Bill does extensively change the rules relating to jurisdiction. Under the 1988 Act the Commissioner has a power to prohibit the transfer of data outside the State where he is of the opinion "that the transfer would, if the place were in a State bound by the Convention, be likely to lead to a contravention of the basic principles for Data Protection set out in Chapter II of the Convention"[64]. The 2002 Bill reduces this power, the Data Protection Commissioner can no longer prohibit transfers of data to States within the EEA. If he wishes to prohibit a transfer he will also have to take into account a range of other issues such as:

> "a) the nature of the data,
> b) the purposes for which and the period during which the data are intended to be processed,
> c) the country or territory of origin of the information contained in the data,
> d) the country or territory of final destination of that information,
> e) the law in force in the country or territory referred to in paragraph (d)
> f) any relevant codes of conduct or other rules which are enforceable in that country or territory,
> g) any security measures taken in respect of the data in that country or territory, and
> h) the international obligations of that country or territory."[65]

However if the EU Commission has decided that a country is a suitable recipient for data then the Data Protection Commissioner is bound by that decision[66]. Much of the decision making power in relation to transfers of data outside the EEA has in effect been transferred to the EU Commission. This means that the 2002 Bill can only have a limited impact on how and when data can be transferred outside the EU. However, this issue is particularly relevant to Ireland given the very high proportion of non-EU multi-nationals which have major operations in Ireland. A review should be undertaken of whether or not Ireland can adapt the provisions of section 10 of the 2002 Bill to take account of the circumstances of these multinationals. This review might be undertaken in the context of the safe harbour principles that have been agreed between the EU and the USA.

Recommendation:

- **A review should be undertaken as to whether Ireland can adapt the provisions of section 10 of the 2002 Bill to take account of the role that non-EU multinationals play in the Irish economy.**

[64] Section11, 1988.
[65] Section 11(1) 1988, as inserted by section10, 2002
[66] Section 11(2) 1988, as inserted by section10, 2002

PART VI - ENFORCEMENT.

Enforcement of Data Protection law is carried out in two ways: firstly the Data Protection Commissioner can enforce it by acting upon complaints; secondly, the individual data subject can enforce Data Protection by seeking access to his or her personal data, raising objections or suing for damages. Arguably, the Data Protection Commissioner has very limited powers of enforcement in comparison with the individual. Since data subjects are not aware of their powers they do not enforce them, but Data Controllers are unwise to assume that just because the Data Protection Commissioner or data subjects do not object now that there is no possible liability for them. Section 7 of the 1988 Act makes it clear that data subjects can sue for damages, although it is difficult to assess at what level the courts would assess damages in a Data Protection case. However, given that appeals from decisions of the Data Protection Commissioner must be taken to the Circuit court, this would seem the logical place in which to issue proceedings in respect of a breach of Data Protection law. The Circuit Court jurisdiction is currently between €6,346.72 and €38,092.14 although this is due to rise to €20,000 and €100,000 with the implementation of the Courts Act 2002. As Data Protection law applies to automated processing this may mean that any breach of Data Protection law may give rise to a very large number of plaintiffs with identical claims and entitled to identical awards for damages. So a bank which interfered with the Data Protection rights of 20,000 of its customers might face a total claim worth between €126 and €761 million. The potential for bringing a very large number of high cost claims means that it is imperative that Ireland should ensure that it is as easy as possible to ensure that Irish firms comply with Data Protection law. One method by which the liabilities of companies might be reduced would be by providing for audits of compliance with Data Protection law. The German Act provides for such audits:

> "With a view to improving data protection and data security, suppliers of data-processing systems and programs and data-processing bodies may have their Data Protection plans and their technical facilities audited and evaluated by independent and licensed experts"

Compliance with Data Protection would obviously be improved by such audits, particularly as a company which was audited would have a very good defence against claims of negligence. If it was decided to introduce such audits, an exemption from liability might be included in the legislation. German law requires the appointment of a Data Protection Officer[67] in all but the smallest companies or public bodies. This officer must have the relevant expertise and need not necessarily be an employee of the company. He must monitor the implementation of Data Protection law and in particular he must:

[67] Germany, Article 4f

1. monitor the proper use of data processing programs with the aid of which personal data are to be processed; for this purpose he shall be informed in good time of plans for the automatic processing of personal data;
2. take suitable steps to familiarise the persons employed in the processing of personal data with the provisions of this Act and other provisions concerning Data Protection and with the particular Data Protection requirements relevant to each case[68]".

Criminal Penalties.

The 1988 Act does contain some criminal penalties for breaches of its provisions, these should be integrated with the implementation of the Cybercrime Convention.

Recommendations:

- **Consideration should be given to the use of Data Protection audits by licensed Data Protection auditors and some statutory exemption from liability for any Data Controller which is so audited;**
- **The appointment of Data Protection officers within firms should also be analysed;**
- **The criminal provisions of the 1988 Act should be integrated with the implementation of the Cybercrime Convention.**

[68] Germany Article 4g.

AFTERWORD:

A comparison of the Data Protection laws of different Member States shows that Ireland has a comparatively lax approach to Data Protection. It is noticeable that the Member States that have the most stringent approach to Data Protection appear frequently to be those that have experienced a dictatorship in the relatively recent past. A good example is Spain, which provides that files of the Spanish security services are subject to the laws of Data Protection[69], and more strikingly provides that:

> "2. Collection and processing, for police purposes, of personal data by the security forces without the consent of the data subjects shall be limited to those cases and categories of data necessary for the prevention of a genuine threat to public safety or for the suppression of crime; such data shall be stored in special files established for the purpose, which must be classified according to their degree of reliability.
> 3. The data referred to in paragraphs 2 and 3 of Article 7 may be collected and processed only in cases in which it is absolutely essential for the purposes of a specific investigation, without prejudice to checks on the legality of the administrative action or the obligation to consider any applications made by the data subjects falling within the remit of the bodies responsible for the administration of justice".

The German Act takes perhaps the broadest approach to Data Protection, it provides in relation to "data avoidance and data economy" that:

> "The organisation and choice of data-processing systems shall be guided by the objective of collecting, processing and using as little personal data as possible. In particular, use shall be made of the possibilities of anonymisation and pseudonymisation where possible and where the effort entailed is proportionate to the interests sought to be protected."

Greece provides extensive provisions that apply to the use of data matching and data mining software. This argument should not be taken too far, the UK has been far more diligent in its implementation of Data Protection law than Ireland. However, it should be kept in mind that Ireland's relatively relaxed approach to Data Protection may be a reflection of Ireland's comparatively stable recent history. Ireland's approach may also reflect the reality that until very recently Ireland was a small, undeveloped economy where comparatively little data processing would have been carried on.

[69] In contrast the Irish Act does not apply to "personal data that in the opinion of the Minister (for Justice) or the Minister for Defence are, or at any time were, kept for the purpose of safeguarding the state".

Ireland is complacent about Data Protection, but it may lose its complacency in the future. As the Irish economy becomes more sophisticated and more deeply integrated into the Information society, it would be surprising if Irish people do not develop greater concerns about the manner in which their personal data is treated. In this regard greater consideration should be given to the implementation of Article 21(1) which provides that:

> "Member States shall take measures to ensure that processing operations are publicized".

Recommendation:

- **More should be done to make Irish people aware of the threats posed to their privacy, such educational work should be targeted at specific groups, individuals should be made aware of how their privacy can be invaded on-line, while companies should be made aware that failure to abide by Data Protection law may expose them to tort liabilities.**
- **A review should be undertaken of how Ireland can publicise the existence of data processing operations in accordance with Article 21 of the Directive.**