FRA

Thematic Legal Study on assessment of data protection measures and relevant institutions [Ireland]

[Dublin][Ireland]
February 2009

Contents

Executive summary

[1]. This report looks into the data protection system which has been built up in Ireland in recent decades. Like many other countries, Ireland has had to adapt its systems for protecting privacy rights, and civil liberties generally, in order to keep pace with changes in technology. This has led to significant legislative changes in recent years, as the legal protections had grown obsolete and were updated. Data privacy is taken seriously by the Irish authorities, and it appears that significant attention will continue to be paid to data protecton issues in the future as well.

[2]. The key institution in this regard is the Data Protection Commissioner, which is established under the Data Protection Acts 1988-2003. These pieces of legislation were designed to ensure that Ireland remains compliant with the corresponding EC Directives on the issue, and it is unsurprising that recent advances here mirror those to be found in other EU Member States. The Office of the Data Protection Commissioner is an independent statutory body whose funding is allocated under the auspices of the Department of Justice, Equality and Law Reform. The Commissioner is appointed by the Government for a renewable term of five years, but is stated by the relevant legislation to be independent in the performance of his/her functions.

[3]. The kind of role the Commissioner should play in the data protection system has been a matter of considerable debate in Irish legal circles, but currently it can be described as that of an enforcer, an ombudsman and an educator. While there have been calls for the Commissioner to be given stronger powers of enforcement and punishment, the current thinking appears to be that more can be achieved by having the Commissioner cooperate with large data controllers to ensure that they are aware of what their data protection responsibilities are, and how best they can meet them.

[4]. The Office of the Data Protection Commissioner plays a multi-faceted role in the overall data protection system in Ireland: from contributing to draft legislation and monitoring violations of current legislation, to hearing complaints and conducting independent investigations. While overall the contribution made by the DPC to data privacy protection in Ireland is laudable, this report finds that there are a great many areas where improvement would be desirable. Most notable amongst these is the Commissioner's level of input into new pieces of draft legislation which potentially impact on data privacy issues. While the DPC has been consulted on some major pieces of legislation, this process is not compulsory for individual Government Departments, and indeed it would appear that some departments view the DPC as a hurdle to be overcome rather than as a body to be cooperated with.

[5]. The other major deficiency with the Irish data protection system identified by this report is the lack of a compulsory data-breach reporting requirement on the various data controllers and processors operating in the jurisdiction. These requirements form a major part of legislation in other jurisdictions, but the absence of an Irish equivalent appears to limit the effectiveness of the DPC, and indeed the legislation in general. Further, there are arguments to suggest that the general public's confidence in the Irish data protection system has been damaged by a series of media reports regarding large-scale data breaches which had been hidden from the public eye for considerable lengths of time.

[6]. The lack of a data-breach reporting requirement has also hampered the ODPC's ability to effectively monitor the levels of compliance with statutory requirements, but has seen the Office develop a useful working relationship with data controllers which sees greater levels of cooperation being reached in this country than in many other jurisdictions. The ODPC has also become proficient at carrying out privacy audits and general investigations on its own initiative or following complaints about specific organisations. A lack of hard data on such investigations means that it is difficult to assess their overall effect, but it would appear that they are a useful weapon in the Commissioner's arsenal. They also complement the ODPC's ombudsman function which sees it hear complaints from all sections of the community, with the possibility of using its broad powers to issue 'enforcement notices' to data controllers who are not complying with the legislation.

[7]. Although recent legislation has sharpened the DPC's teeth as regards punishing certain kinds of organisations who fail to comply with statutory requirements, much of its work revolves around increasing awareness of data privacy rights and responsibilities. That the DPC maintains a positive profile with both individuals and organisations is clear from the popularity of its website and helpdesk as sources for data protection information. The DPC also runs various initiatives aimed at increasing awareness of data privacy issues amongst key groups – such as employers, employees and young people. The effects of this part of the Commissioner's work are highlighted in the largely positive results of the Public Awareness Survey carried out on behalf of the Commissioner during 2008.

[8]. Overall, this report shows that the Irish data protection system is not perfect but that it has numerous good points which could be used to inspire similar systems elsewhere in the Union. Some of the major deficiencies in the Irish system are currently under review so progress may be expected in those areas, but the budget of the DPC is due to be cut by almost one-tenth in the next year, so the Irish data protection system may see further challenges in its future too.

1. Overview

[1]. Although there is no express reference to a right to privacy in the Irish Constitution, the Supreme Court has ruled that an individual may invoke the personal rights provision in Article 40.3.1 to establish an implied right to privacy.[1] This article provides, "The State guarantees in its laws to respect, and, as far as practicable, by its laws to defend and vindicate the personal rights of the citizens." It was first used to establish an implied constitutional right in the case of McGee v. Attorney General[2], which recognized the right to marital privacy. This case has been followed by others such as Norris v. Attorney General[3] and Kennedy and Arnold v. Ireland[4]. In the latter case, the Supreme Court ruled that the illegal wiretapping of two journalists was a violation of the constitution, stating:

[2]. "The right to privacy is one of the fundamental personal rights of the citizen which flow from the Christian and democratic nature of the State . . . . The nature of the right to privacy is such that it must ensure the dignity and freedom of the individual in a democratic society. This can not be insured if his private communications, whether written or telephonic, are deliberately and unjustifiably interfered with."

[3]. In 1988, the Data Protection Act[5] was passed to implement the 1981 Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data[6]. The Act regulates the collection, processing, keeping, use and disclosure of personal information processed by both the private and public sectors. However, before its amendment, the Act applied only to information automatically processed. Under it individuals have a right to access and correct inaccurate information. Such information can only be used for specified and lawful purposes and cannot be improperly used or disclosed. Additional protections can be ordered for sensitive data. Criminal penalties can be imposed for violations. There are broad exemptions for national security, tax,

[1] Bunreacht na hEireann 1937 (Irish Constitution), available at http://www.taoiseach.gov.ie/attached_files/html%20files/Constitution%20of%20Ireland%20(Eng)Nov2004.htm, last accessed 11.01.09.
[2] 1974 I.R. 284
[3] 1984 I.R. 36
[4] 1987 I.R. 587
[5] Act No 25 of 1988, available at http://www.irishstatutebook.ie/1988/en/act/pub/0025/sec0009.html#zza25y1988s9, last accessed 08.01.09.
[6] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28.01.81, available at http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm, last accessed 08.01.09.

and criminal purposes. Misuse of data is also criminalized by the Criminal Damage Act 1991[7].

[4]. As a member of the European Union, Ireland should have amended this Act and extended its scope to implement the European Data Protection Directive by October 1, 1998. In January 2000, the European Commission initiated a case before the European Court of Justice against Ireland and four other countries for failure to implement the Directive on time[8]. In December 2001, certain provisions of the Directive were implemented by the European Communities (Data Protection) Regulations, 2001[9]. The regulations took effect in April 2002 and governed the transfer of personal information to third countries (i.e. non-European Economic Area countries). The Data Protection (Amendment) Act 2003[10] (the Act) was finally enacted in July 2003, repealing the regulations and purporting to give effect to the EU Data Protection Directive.

[5]. As will be seen below in detail, the Act amended the existing law in several ways. The definition of "data" was extended to manual as well as automated files. The Act also broadened the definition of "processing" to performing "any" operation on the data[11]. The rights of individuals in the areas of notice, access and consent were also improved. Section 6B, as inserted by the 2003 Act, introduced a right in relation to automated decision making. It provides that decisions that significantly affect a data subject (such as work performance, creditworthiness, reliability or conduct) may not, in the absence of consent, be taken automatically without human input.

[6]. The Act also clarifies, and in many cases increases, the responsibilities of data controllers. It provides additional protection for "sensitive" data, defined as information relating to racial or ethnic origin, political opinions, religious or philosophical belief, trade union membership, physical or mental health, sexual life, the commission or alleged commission of an offence and any subsequent proceedings[12]. Except in extreme circumstances, data controllers must get explicit consent before processing sensitive data, and must provide additional safeguards[13].

[7]. The Data Protection (Amendment) Act also provides for a number of measures concerning those involved in direct marketing. Under previous data protection

[7] Section 5, Criminal Damage Act 1991. Act No 31 of 1991, available at http://www.irishstatutebook.ie/1991/en/act/pub/0031/index.html, last accessed 12.01.09.
[8] European Commission, Press Release, "Data Protection: Commission Takes Five Member States to Court," January 11, 2000
[9] S.I. No. 626/2001 — European Communities (Data Protection) Regulations, 2001, available at http://www.irishstatutebook.ie/2001/en/si/0626.html, last accessed 12.01.09.
[10] Act No 6 of 2003, available at http://www.irishstatutebook.ie/2003/en/act/pub/0006/index.html, last accessed 08.01.09. An informal consolidation of the legislation is available at http://www.dataprotection.ie/viewdoc.asp?DocID=796&ad=1, last accessed 12.01.09.
[11] Section 2(a)(v) DPA 1988-2003.
[12] Section 2(a)(i) DPA 1988-2003.
[13] Section 2B as inserted by the 2003 Act.

legislation, information garnered from sources required by law to be publicly available (such as the electoral register) was exempt. Under the 2003 Act, an individual now has the right to object to use of this data for direct marketing purposes, and the controller must inform the individual of this right. In addition, the Electoral Amendment Act 2001 makes provision for the establishment of an edited electoral register similar to a system already deployed in the United Kingdom. Local authorities must now prepare two versions of the electoral register, a full one that can only be used for electoral and statutory purposes, and an edited version that will contain the names and addresses of those who have indicated their willingness to be contracted by commercial entities[14]. It is an offence to use information on the Full Register for non-electoral or non-statutory purposes[15]. Data controllers may only process the details of those persons published on the Edited Register for purposes other than an electoral or other statutory purpose.

[8]. As a full member of the United Nations since 14 December 1945, there is also a base level of privacy protections guaranteed in the Irish State by virtue of UN Human Rights pronouncements. Ireland has ratified the core UN human rights treaties and a wide range of other international human rights instruments[16]. In particular the text of Article 12 of the UN Declaration of Human Rights guarantees that "[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation"[17]. This sentiment is echoed in Article 17 of the International Covenant on Civil and Political Rights of 16 December 1966, which Ireland signed in 1983 and then ratified in December 1989[18]. In its Third National Report[19] under the ICCPR the State emphasized the role of the Data Protection Commissioner in enduring its compliance with these provisions, but it did note the concern raised on a national level by proposals to include provisions for biometric data systems in the Privacy Bill under consideration at the time.

[9]. Generally speaking, Ireland is said to have a reasonably comprehensive system of data privacy protections, and is seen as being broadly in line with international best practices in the area. The key institution in this regard is, of course, the office of the Data Protection Commissioner, but its work is supplemented by some hard-working (but perpetually underfunded) interest groups in the area. Most notable amongst these is the independent civil liberties

[14] Section 4 DPA 1988-2003

[15] Under Section 13A(3) of the Electoral Act, 1992 (as amended by the Electoral (Amendment) Act, 2001). Act No 23 of 1992, available at http://www.irishstatutebook.ie/1992/en/act/pub/0023/index.html, last accessed 12.01.09.

[16] Full list available on http://www.dfa.ie/home/index.aspx?id=318, last accessed 12.03.09

[17] Full text available at http://www.un.org/Overview/rights.html, last accessed 12.03.09

[18] See list of ratifications on: http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&id=322&chapter=4&lang=en, last accessed 12.03.09.

[19] Available at http://www.dfa.ie/uploads/documents/Political%20Division/iccprfinalpdf.pdf, last accessed 12.03.09.

group *Digital Rights Ireland*[20], whose website provides a valuable alternative source of information regarding data protections in Ireland. The group is led by Mr Thomas McIntyre[21], a lecturer with the School of Law at University College Dublin, and is in the process of taking a high-profile case against the State to challenge the Government's data retention policies[22]. This group is the leader amongst the civil society organisations operating in the area, and possesses important links with similar bodies in other jurisdictions which facilitates easy comparisons to be drawn between Ireland and other European countries especially.

[10]. There is continuing debate in Ireland about the form the Data Protection Commissioner's office should take – with many vocal critics suggesting that the current ombudsman/facilitator model should be sidelined in favour of a watchdog/enforcer body along the lines of the Information Commissioner's Office in the United Kingdom. Notwithstanding this debate, the Irish Data Protection Commissioner maintains a good reputation in Irish legal circles, and is noted for its good working relationships with the interested parties in the area. As will be examined in detail below, the Commissioner uses this good relationship to work with industry players to foster a tradition of cooperation which, it is hoped, will lead to greater levels of compliance than tough enforcement alone could achieve.

[11]. That is not to say that considerable deficiencies do not persist in the Irish system. The main underlying weakness in the Irish system is the lack of a legal compulsion on Irish data controllers to report all breaches to the DPC. This is also discussed at length below, and changes may well be afoot in this regard, but there is little doubt that public confidence in the data privacy protections has suffered in Ireland in recent years in light of a series of media reports about large data-breaches that were hidden form the public by both State-run and private organisations. In recent months the Government has formed a high-level group of experts (including the current DPC) to investigate whether legislation is need to fill this gap. Although significant damage has already been done, the willingness of the Government to take steps to fill the remaining gaps in the system is encouraging, and shows a sense of recognition of the importance of data privacy issues overall.

[20] See further: www.digitalrights.ie, last accessed 29.01.09
[21] See further: http://www.tjmcintyre.com, last accessed 29.01.09
[22] See further: http://www.mcgarrsolicitors.ie/2006/09/08/digital-rights-ireland-data-retention-case/, last accessed 29.01.09

2. Data Protection Authority

[1]. The Data Protection Commissioner (DPC) was originally established by Section 9(1) of the Data Protection Act 1988[23], pursuant to the Strasbourg Convention of 1981[24]. The Commissioner's office and functions were redefined and reinvigorated by Directive 95/46[25] which set down that independent national supervisory authorities are an essential component of the protection of individuals with regard to the processing of their personal data[26]. This Directive led to the Data Protection (Amendment) Act 2003[27], and although the DPC was already in possession of many of the powers required by the Directive, the 2003 Act did make some important changes. As detailed below the Commissioner may now undertake investigations on his/ her own initiative, check certain processing operations before they commence, and his/ her annual report benefits from absolute privilege for the purposes of defamation law.

[2]. Under the Data Protection Acts 1988-2003 (DPA) the DPC is a body corporate and is stated to be "…independent in the performance of his functions[28]". He or she is appointed by the Government and holds office upon terms and conditions determined by the Government. The DPC's term of office is 5 years, although they may be reappointed and their term can be curtailed should they resign or reach the age of 65 years. The Commissioner can also be removed from office by the Government if, in the opinion of the Government, he/she has become "incapable through ill-health of effectively performing their functions or has committed stated misbehaviour[29]".

[23] Act No 25 of 1988, available at http://www.irishstatutebook.ie/1988/en/act/pub/0025/sec0009.html#zza25y1988s9, last accessed 08.01.09.

[24] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28/01/81, available at http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm, last accessed 08.01.09.

[25] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, available at http://eur-lex.europa.eu/Notice.do?val=307229:cs&lang=en&list=307229:cs,&pos=1&page=1&nbl=1&pgs=10&hwords=95/46/EC~&checktexte=checkbox&visu=#texte, last accessed 08/01/09.

[26] Directive 95/46 Recital 62, available at http://www.dataprotection.ie/viewdoc.asp?DocID=91, last accessed 08.01.09.

[27] Act No 6 of 2003, available at http://www.irishstatutebook.ie/2003/en/act/pub/0006/index.html, last accessed 08.01.09.

[28] DPA Schedule 2, paragraph 1, available at http://dataprivacy.fusio.net/docs/Data_Protection_Act_1988_-_1st_2nd_3rd_Schedules/67.htm, last accessed 08.01.09.

[29] DPA Schedule 2, paragraph 2(2)(b), available at http://dataprivacy.fusio.net/docs/Data_Protection_Act_1988_-_1st_2nd_3rd_Schedules/67.htm, last accessed 08.01.09.

[3]. The Office of the Data Protection Commissioner is part of the State's family of human rights agencies with the particular right they help to uphold being the right to privacy. Its functions under the Data Protection Acts and related legislation fall into 3 main categories: **Ombudsman Role**: resolution of disputes between individuals and data controllers or processors; **Enforcer Role:** compliance by data controllers and processors; **Educational Role:** Promoting data protection rights and good practice.

[4]. In its ombudsman role, its focus is on achieving mediated solutions, where possible. Complaints offer insight into the concerns of people, and help to guide the educational activities of the Office. The educational role of the Office is a broad one. It encompasses everything from public information campaigns, to targeted advice to particular companies, to private discussions with Government agencies on new legislative proposals. Educating people on their right to data privacy is considered important because only if people know their rights can they take effective measures to vindicate them. The objective of the DPC is that, through greater awareness of data protection rights, people will be empowered to protect their own privacy. The DPC works with different sectoral groups and tries to build privacy protection into policy proposals at an early stage. Working with government agencies and commercial bodies at an early stage means that privacy protection can be part of the solution and not - as it is sometimes presented – a barrier to progress.

[5]. The powers granted to the DPC under the 1988 and 2003 Acts were designed to bring it into line with the requirements set down in Article 28 of Directive 95/46/EC. Under section 10 of the Data Protection Acts, 1988 and 2003, the Commissioner will investigate any complaints which he/ she receives from individuals who feel that personal information about them is not being treated in accordance with the Act, unless he/she is of the opinion that such complaints are "frivolous or vexatious". The Commissioner notifies the complainant in writing of his/ her decision regarding the complaint. The Commissioner's decision can be appealed to the Circuit Court.
The Commissioner's approach to complaints, as provided under the Acts, is to try to reach an amicable resolution to the matter which is the subject of the complaint. In cases where it is not possible to reach an amicable resolution, a complainant may ask the Commissioner to make a formal decision as to whether a contravention has occurred. However, the Commissioner does not have the power to award compensation. The Commissioner's main priority, if he/ she upholds a complaint, is that the data controller complies with the law and puts matters right. If an individual suffers damage through the mishandling of their personal information, then they may be entitled to claim compensation through the Courts but the Commissioner has no function in relation to the taking of such proceedings or in the giving of legal advice.

[6]. Under section 12 of the Data Protection Acts, 1988 and 2003, the Data Protection Commissioner may require any person to provide him/ her with whatever information the Commissioner needs to carry out his/ her functions,

such as to pursue an investigation. The Commissioner exercises this power by providing a written notice, called an "information notice", to the person. A person who receives an information notice has the right to appeal it to the Circuit Court.
Failure to comply with an information notice without reasonable excuse is an offence. Knowingly to provide false information, or information that is misleading in a material respect, in response to an information notice is an offence. No legal prohibition may stand in the way of compliance with an information notice. The only exceptions to compliance with an information notice are (i) where the information in question is or was, in the opinion of the Minister for Justice, Equality and Law Reform, or in the opinion of the Minister for Defence, kept for the purpose of safeguarding the security of the State, and (ii) where the information is privileged from disclosure in proceedings in any court.

[7]. Under section 10 of the Data Protection Act, 1988, the Data Protection Commissioner may require a data controller or data processor to take whatever steps the Commissioner considers appropriate to comply with the terms of the Data Protection Act, 1988. Such steps could include correcting the data, blocking the data from use for certain purposes, supplementing the data with a statement which the Commissioner approves, or erasing the data altogether. The Commissioner exercises this power by providing a written notice, called an "enforcement notice", to the data controller or data processor. A person who receives an enforcement notice has the right to appeal it to the Circuit Court. It is an offence to fail or refuse to comply with an enforcement notice without reasonable excuse.

[8]. Under section 11 of the Data Protection Acts, 1988 and 2003, the Data Protection Commissioner may prohibit the transfer of personal data from the State to a place outside the State. The Commissioner exercises this power by providing a written notice, called a "prohibition notice", to the data controller or data processor. In considering whether to exercise this power, the Commissioner must have regard to the need to facilitate international transfers of information. A prohibition notice may be absolute, or may prohibit the transfer of personal data until the person concerned takes certain steps to protect the interests of the individuals affected. A person who receives an enforcement notice has the right to appeal it to the Circuit Court. It is an offence to fail or refuse to comply with a prohibition specified in a prohibition notice without reasonable excuse.

[9]. Under section 24 of the Data Protection Acts, 1988 and 2003, the Data Protection Commissioner may appoint an "authorised officer" to enter and examine the premises of a data controller or data processor, to enable the Commissioner to carry out his/her functions, such as to pursue an investigation. The authorised officer, upon production of his or her written authorisation from the Commissioner, has the power to:

- enter the premises and inspect any data equipment there;
- require the data controller, data processor or staff to assist in obtaining access to data, and to provide any related information;
- inspect and copy any information;
- require the data controller, data processor or staff to provide information about procedures on complying with the Act, sources of data, purposes for which personal data are kept, persons to whom data are disclosed, and data equipment on the premises.

It is an offence to obstruct or impede an authorised officer; to fail to comply with any of the requirements set out above; or knowingly to give false or misleading information to an authorised officer.

[10]. As a statutory body, the remit of the DPC is limited to investigating breaches of the DPA: under Section 10(1) of the DPA he/ she "may investigate, or cause to be investigated, whether any of the provisions of this Act have been, are being or are likely to be contravened in relation to an individual either where the individual complains to him of a contravention of any of those provisions or he/she is otherwise of opinion that there may be such a contravention."

[11]. The DPC's staff are civil servants, and the DPC must maintain accounts which may be audited by the Comptroller and Auditor General. The current Commissioner, Mr Billy Hawkes, was appointed in April 2005 and now has a staff of 22 with a budget of €1,835,375 in 2007[30]. When compared to similar institutions in other European countries the DPC is relatively well funded, although they are set to have their budget cut by 9% this year in line with general cutbacks across the whole 'justice family'[31]. A further problem encountered by the DPC is that its staff is made up of generalist civil servants allocated through the central appointments system, and it is felt that if the Commissioner had independent powers of recruitment it would be easier for him to attract legal and IT professionals with specialist skills relevant to the function of the Office.

[12]. Article 28(1) of Directive 95/46 requires the DPC to act with complete independence in exercising the functions entrusted to him, and although the DPA states the Commissioner to be independent, this has been called into question in the past. During the drafting of the original 1988 Act the then Minister for Justice described the DPC's role as "more of a mediator" who could "help those who keep personal data to bring their operating procedures

[30] Annual Report of Data Protection Commissioner 2007, available at http://dataprivacy.fusio.net/viewdoc.asp?Docid=721&Catid=50&StartDate=1+January+2009&m=p, last accessed 08.01.09.

[31] See http://www.irishtimes.com/newspaper/frontpage/2008/1212/1229035603353.html, last accessed 29.01.09

into line with the Act[32]". However, the clear statement of functional independence used in the Directive, and subsequently the 2003 Act, has removed any doubt about the role of the DPC.

[13]. Although the Commissioner is independent, his/her decisions are still subject to review by the courts. Under section 26 of the Data Protection Acts, appeals can be made to the Circuit Court against:

- a requirement specified in an information notice;
- a requirement specified in an enforcement notice;
- a prohibition specified in a prohibition notice;
- a refusal by the Data Protection Commissioner to accept an application for registration, or for renewal of registration, or for an amendment of registration details; or
- a decision of the Data Protection Commissioner in relation to a complaint by an individual.

Appeals to the court must normally be made within 21 days from the service of the notice, or from the data of receipt of the refusal or decision. The decision of the court is final, although an appeal against the court's decision may be brought to the High Court on a point of law.

[14]. Overall, the ODPC operates without interference from other branches of Government, even though it remains reliant on the Depatment of Justice, Equality and Law Reform for its funding. The guarantees of independence contained in the legislation ensure that it can operate according to its own agenda, and also help it to maintain an independent public image – which is important as it tries to raise awareness of its own role as well as data privacy issues generally. The fact that it is subject to review by the courts does not prevent it from making effective use of the powers granted to it, and indeed this fact may well inspire greater confidence in it amongst the general public, thereby further enhancing its public image.

[15]. As regards activities undertaken by the DPC on his/her own initiative, the most notable are the investigations and audits carried out every year. Sections 10 (1A) and (1B) of the Data Protection Acts provide that: "The Commissioner may carry out or cause to be carried out such investigations as he or she considers appropriate in order to ensure compliance with the provisions of this Act and the Electronic Communications networks and Services Regulations of 2003 and to identify any contravention thereof."

[32] Gerard Collins, Minister for Justice, Dail Eireann – Volume 375 – 17 November 1987 – Data Protection Bill 1987: Second Stage, available at http://historical-debates.oireachtas.ie/D/0375/D.0375.198711170154.html, last accessed 08.01.09.

[16]. These investigations usually take the form of audits of selected organisations. A number of such audits are carried out each year. The aim of an audit is to identify any issues of concern about the way the organisation deals with personal data and to recommend solutions. Such audits are supplementary to specific investigations carried out following individual complaints, and allow the DPC to take a more proactive role in key areas where data protection concerns exist.

[17]. An organisation selected for audit is usually given a number of week's notice of the audit. It may be asked to provide in advance a written report on its data protection practices. The audit normally includes one or more on-site visits by an audit team from the Office. During these visits, the team will meet with selected staff of the organisation. They will also usually inspect electronic and manual records. At the end of the audit, the team prepares a report which typically includes a set of recommendations. The organisation audited is given an opportunity to comment on this before it is finalised. The Office may follow up later on how these recommendations have been acted on. Under section 24 of the Data Protection Acts, 1988 and 2003, the Data Protection Commissioner may appoint an "authorised officer" to enter and examine the premises of a data controller or data processor and it is an offence to obstruct or impede such authorised officers or to knowingly give false or misleading information to an authorised officer. Once the investigation/audit process has begun the DPC retains control over the direction in which it goes, so he/she can shift its focus to different sectors or departments should the need arise. It is difficult, looking back, to assess how proactive the Commissioner is in the use of such powers but the flexibility built into these competences do appear to leave room for considerable discretion and independent action on the Commissioner's part.

[18]. As regards monitoring violations of data protection legislation, the task of the DPC is very difficult due to the lack of an obligation on data-controllers to report data breaches. The ODPC is not aided by the sheer scale of the operations which it must attempt to monitor, and the relatively scarce resources with which it must do it, but it has developed some innovative ways of encouraging both members of the public and industry players to report their concerns to it. One of the ODPC's main monitoring tools is its well-publicised Helpdesk which provides interested parties with accurate and practical advice on data privacy issues, while at the same time offering the DPC a good insight into the problems being faced by both data subjects and data controllers.

[19]. According to their most recent Annual Report, their helpdesk responded to approximately 20,000 phone enquiries, together with over 4,000 email enquiries and a smaller number of contacts by post. This large number of queries is partly a result of effective education and awareness-raising exercises and increasing numbers of audits and inspections. However, it also reflects the strong and very valuable media profile built up by the Office of the Data Protection Commissioner as journalists engage with privacy issues as a matter of major public concern. This carefully managed profile helps the DPC to attract

correspondence from all sectors of society so that it can effectively monitor the overall level of data protection and detect privacy concerns as they arise.

[20]. The DPC is also proactive in its wide use of privacy audits which are used to assist data controllers to ensure that their data protection systems are sufficient. Priorities for holding such audits are set taking into account the complaints and enquiries made to the Office by members of the public. In addition to these audits the DPC continues to run a program of random inspections in particular industries – most notably in the mortgage brokerage/estate agency sectors following the considerable public concerns raised by a Prime Time Investigates television show aired on RTE in December 2006.

[21]. While there has been criticism of the Commissioner's relatively weak powers to compel data-controllers to come to him/her with any privacy issues, it has had the result of forcing the Commissioner to develop more innovative ways of monitoring the area – most notably by proactively pursuing suspect organisations while simultaneously building good working relationships with the general public to try and ensure that major problems are brought to the ODPC's attention as quickly as possible.

[22]. The website of the DPC includes a comprehensive list of Case Study reports which detail how the Commissioner learned of a problem, what course he/she pursued in investigating it, and the eventual outcome of the process. These Case Studies are used not only to highlight the kinds of privacy problems encountered by the Commission, but they also serve as examples of the kind of conduct expected from data controllers across the country. In his most recent Annual Report the Commissioner, safe in the knowledge that such reports are absolutely privileged for the purposes of defamation law, has begun to publish a complete list of those occasions where he had to resort to the use of legal powers to advance an investigation.

[23]. Where a complaint is made about a breach of the Data Protection Acts, the Commissioner first tries to find a solution that both the parties can accept, and the Office then contacts the individual to ask if they are satisfied with the suggested solution. In cases where an amicable resolution or an informal settlement of the complaint cannot be reached, the Data Protection Commissioner will make a full investigation of all the facts before making his/her Decision. When the investigation is finished, and the Commissioner has reached his/her conclusions, he/she writes to the complainant informing them of his/her Decision. Similarly, if the Commissioner does not uphold a complaint, he/she will inform the complainant of this in writing.

[24]. The Article 29 Working Party is seen by the DPC as the primary method of coordination and cooperation between EU data protection authorities. In recent years the Office of the DPC has placed a particular focus on increasing its contribution to the work of the Article 29 Working Party. It has formally joined and sought to influence the thinking of sub-groups dealing with the sensitive

issue of the treatment of medical data and the challenges posed by developing technology. Its objective is to ensure that the outcomes of discussions take full account of its views and are therefore easier for them to explain and implement domestically. The DPC intends that their contribution to this work will increase systematically over time to ensure that they can both influence and be influenced in their domestic focus by discussions at EU level. Although such activities are very resource intensive for a relatively small office, the Commissioner has stated himself to be more than satisfied that the effort, in terms of the impact on the privacy landscape here, will be rewarded.

[25]. The DPC has traditionally placed great importance on the consensus of opinions reached at the Article 29 Working Party, and uses them to guide and shape the actions it takes in particular areas at domestic level. This is very clear from the approach taken by the ODPC as regards proposals for a National Electronic Health Database which uses a Working Party document[33] as a key reference point.

[26]. The DPC does not have a role in the framing of legislation – nobody has, save for the *Oireactas* (Parliament)[34]. This was acknowledged by the DPC in his 2002 Annual Report[35] as being a necessary result of the fact that his office is a statutory creation. Although not a framer of legislation, the observations of the DPC are regularly sought by government Departments when matters concerning data protection arise in any draft pieces of legislation. The DPC places a particular emphasis on ensuring that data protection requirements can be seen by all as part of a solution to problems rather than an extra barrier to cross. It is the Commissioner's strong preference that data protection issues should be addressed when proposals are at an early stage rather than have problems emerge later when change may be more difficult. Many Government departments and agencies consult the Office of the DPC when developing proposals which may have data protection and privacy implications and the Commissioner continues to devote resources to the identification of privacy-friendly solutions in this context. The experience of the DPC, according to his most recent Annual Report, is that it is usually possible to arrive at solutions which achieve Government objectives while minimising negative impacts on privacy. He is, however, disappointed that some parts of the Government

[33] Working Document on the processing of personal data relating to health in electronic health records, adopted 15.02.07, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_en.pdf, last accessed 19.01.09.

[34] See Article 15.2 of the Irish Constitution (Bunreacht na hEireann 1937, available on http://www.taoiseach.gov.ie/upload/static/256.htm, last accessed 09.01.09)

[35] Available at http://www.dataprotection.ie/viewdoc.asp?Docid=61&Catid=50&StartDate=1+January+2009&m=p, last accessed 09.01.09.

system seem to view his Office with caution in terms of consultation on new proposals[36].

[27]. For example, the Office of the DPC was consulted by the Department of Justice, Equality and Law Reform on the scheme for the Criminal Justice (Forensic Sampling and Evidence) Bill 2007, which was subsequently published by the Department[37]. The Bill provides for the establishment of a database of DNA 'profiles' extracted from samples taken from individuals or collected from crime scenes. The purpose of the database is to assist in crime detection. The DPC highlighted that it is important that the collection and retention of DNA samples and 'profiles' is proportionate and does not interfere unduly with the individual's right to data privacy. The Commissioner went on to suggest that the Government consider amending the Bill to provide for the destruction of samples and profiles of persons who have not been found guilty of an offence, in line with the recommendation of the Law Reform Commission[38] on this point.

[28]. The Office of the DPC sees awareness raising and training as a major part of their function, and constantly works towards ensuring that both data subjects and controllers/processors know their rights and responsibilities under the Data Protection Acts. Indeed, the Commissioner sees increasing awareness and understanding of data protection issues amongst the public and those entities holding personal data as being mutually beneficial[39].

[29]. As regards organisations, the DPC has developed a range of materials explaining how the DPA can apply to the day-to-day activities of various businesses and agencies. The Office of the DPC also provides training materials and programs to help employers to explain DPA requirements to their employees. The desire on the part of organisations to avail of formal data protection training is dramatically increasing and the Office receives a large number of queries about such training. While they are not in a position to offer formal training as such, they do seek to assist through presentations at appropriate events and training supports available through their website[40], including useful DVD/You-Tube resources. Beyond that they actively collaborate with a number of organisations in the development of formal data protection courses and events. The Commissioner views these developments as

[36] 2007 Annual Report, page 22, available at http://www.dataprotection.ie/documents/annualreports/AR2007En.pdf, last accessed 09.01.09.
[37] Available at http://www.justice.ie/en/JELR/Pages/PB07000497, last accessed 09.01.09.
[38] "The Establishment of a DNA Database", Law Reform Commission, Report LRC 78-2005, November 2005 at www.lawreform.ie, last accessed 09.01.09.
[39] 2007 Annual Report, page 20, available at http://www.dataprotection.ie/documents/annualreports/AR2007En.pdf, last accessed 09.01.09.
[40] Available at http://www.dataprotection.ie/ViewDoc.asp?fn=%2Fdocuments%2FTrainingAndAwareness%2Ehtm&CatID=95&m=t, last accessed 09.01.09.

extremely worthwhile since they will further develop an understanding of data protection requirements.

[30]. As regards individuals, the same part of the DPC website provides links to booklets and PowerPoint presentations outlining the protections offered by the DPA and what an individual should do if their rights are not being respected. A 2005 awareness survey conducted on behalf of the Office of the DPC found that 18 - 24 year olds display some of the lowest levels of awareness and knowledge of personal privacy issues and, further, that they regard such issues as having a low level of importance. In response to this finding, the Commissioner specifically targeted younger people in 2007 by engaging extensively with people of school going age to identify issues that impact on their privacy. The Commissioner then embarked on a series of visits and presentations to schools, and a new resource book targeted at junior cycle Civic, Social and Political Education (CSPE) secondary school students was devised. The resource was entitled 'Sign-Up, Log In, Opt Out: Protecting your Privacy & Controlling your Data' and was made available via the DPC website.

[31]. More generally the Commissioner hosts industry-specific seminars to raise awareness and prompt discussion, most notably within the health sector where the focus was on key privacy issues associated with health research. The DPC also regularly contributes to the broadcast and print media as data protection issues arise. This is seen a key opportunity to promote awareness so the Office has an active policy of making themselves available to the media when requested to do so. Another notable publicity campaign launched by the DPC concerned the direct marketing aspect of the Electoral Register and the facility to 'opt out'. It was run in conjunction with the Commission for Communications Regulation (ComReg) and consisted of national newspaper and radio advertisements.

3. Compliance

[1]. With effect from 01.10.2007, the following categories of data controller are required to register with the Data Protection Commissioner if they hold or process personal data on computer:

- Government bodies / public authorities;
- banks, financial / credit institutions and insurance undertakings;
- persons whose business consists wholly or mainly in direct marketing, in providing credit references or in collecting debts;
- internet access providers;
- telecommunications network or service providers;
- anyone processing personal data related to mental/physical health or genetic data; and
- anyone whose business consists of processing personal data for supply to others, other than for journalistic, literary or artistic purposes.

[2]. Data processors who process personal data on behalf of a data controller falling under any of the categories listed above are also required to register with the Data Protection Commissioner. If a data controller or data processor is obliged to register with the Office of the Data Protection Commissioner, it is an offence to continue to process data while unregistered. The Act provides for fines of up to €3,000 on summary conviction. The DPC has made it possible to complete the renewal process online and pay by Laser, Mastercard or Visa.

[3]. In 2007 the number of organisations registered decreased by 681 or 10.7%. The decrease is a result of the implementation of the new registration regulations (S.I. No. 657 of 2007) after 01.10. 2007. Changes in the requirement to register in the education and legal profession sectors contributed most to the decrease. The categories of data controller which were previously required to register but no longer have to do so include: not-for-profit organisations; elected representatives and candidates for electoral office; educational institutions; solicitors and barristers - provided they do not also fall within one of the categories of those who are still required to register. A comprehensive list of registrations currently held by the Office of the DPC is available online[41], and is updated regularly.

[41] Available at http://www.dataprotection.ie/docs/Current_list_of_Registrations_held_by_the_Data_Protection_Co/8.htm, last accessed 10.01.09.

[4]. The requirement for registration is part of an effort to supervise the retention of personal data, in the interests of those people whose data are being stored. In summary, data controllers are under a duty to ensure that data is:

- Obtained and processed fairly;
- Kept only for one or more specified lawful purposes;
- Processed in ways compatible to the purposes for which it was supplied initially;
- Kept safe and secure;
- Not disclosed to third parties except where it is appropriate to do so;
- Kept accurate and up to date;
- Adequate, relevant and not excessive; and
- Retained for no longer than is necessary.

In addition, a copy of the data must be provided, on request, to the individual to whom it refers. The individual has the right to have this data corrected, if it is inaccurate, or erased, if the data controller does not have a legitimate reason for retaining it.

[5]. Sensitive personal data relates to specific categories of data which are defined as data relating to a person's racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life; criminal convictions or the alleged commission of an offence; trade union membership. To fairly process sensitive data it must firstly have been fairly obtained and additional special conditions must be met. The data subject (or their parent/guardian) must have given explicit consent to the processing, or the processing must be necessary for one of the following reasons -

- for the purpose of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment;
- to prevent injury to the health of the data subject or another person, or serious loss in respect of property of the data subject or of another person, where consent cannot reasonably be obtained or is being unreasonably withheld;
- it is carried out by a not for profit organisation in respect of its members or other persons in regular contact with the organisation;
- the information being processed has been made public as a result of steps deliberately taken by the data subject;

- for the purpose of obtaining legal advice, or in connection with legal proceedings, or is necessary for the purposes of establishing, exercising or defending legal rights;
- for medical purposes;
- it is carried out by political parties or candidates for election in the context of an election; or
- for the purpose of the assessment or payment of a tax liability or the administration of a Social Welfare scheme.

[6]. Under the DPA it is also necessary for data controllers to publish a privacy policy if their website does any of the following:

- Collects personal data (visitors filling in web forms, feedback forms, etc.);
- Uses cookies or web beacons; or
- Covertly collects user data (IP addresses, e- mail addresses), which may or may not identify an individual.

The privacy policy must be accessible from all points of the site where personal data is collected. This statement should detail what personal data is collected by the site, and the purpose for which it is collected. The Data Protection Commissioner has published guidelines on such privacy statements. The suggested solution is to place a link to the privacy statement on each page. Alternatively, a link could be placed on any page on which data is collected, although if the website uses cookies, this could mean all pages.

[7]. The ODPC has made it clear, in its guidance literature circulated to organisations[42], that they must make themselves aware of their data protection responsibilities, in particular, to process personal data fairly. Their guidelines state that such organisations must ensure that their staff are made aware of their responsibilities through appropriate induction training with refresher training as necessary and the availability of an internal data protection policy that is relevant to the personal data held by them. An internal policy which reflects the eight fundamental data protection rules and applies them to your organisation, which is enforced through supervision and regular review and audit, is described as a valuable compliance tool. Although specialist data officers do not appear to be required by law, they are greatly encouraged as a way of ensuring that each organisation/department has someone who has taken responsibility for compliance.

[8]. The sheer number of requests for further data protection training received by the DPC would appear to suggest that data controllers are taking their duties under

[42] A Guide for Data Controllers, available at http://www.dataprotection.ie/ViewDoc.asp?fn=/documents/guidance/Guide_Data_Contollers.htm&CatID=90&m=y, last accessed 12.01.09.

the legislation seriously. Although the Commission is severely limited in the amount of training it can provide, there are a great many 'compliance specialists' who offer data protection consultations to Irish data controllers/processors. While the dramatic increase in the amount of complaints received by the ODPC in recent years could be due to more organisations simply failing to comply with the legislation, it would appear that a significant portion of this increase is due to the recently introduced Electronic Communications Regulations as well as the ever increasing media profile of the DPC and privacy rights in general.

[9]. In light of the absence of obligatory data-breach reporting it is difficult to ascertain exact compliance rates, but because the ODPC maintains quite a good working relationship with data controlling organisations it would appear that the majority of such breaches are actually reported to the Commissioner. This would suggest that compliance rates are acceptable, although criticism of the scale and scope of the enforcement powers of the Commissioner remains[43].

[43] E.g. http://www.mulley.net/?s=data+protection+commission+, last accessed 12.01.09.

4. Sanctions, Compensation and Legal Consequences

[10]. Under section 10 of the Data Protection Act, 1988, the Data Protection Commissioner may require a data controller or data processor to take whatever steps the Commissioner considers appropriate to comply with the terms of the Data Protection Act, 1988. Such steps could include correcting the data, blocking the data from use for certain purposes, supplementing the data with a statement which the Commissioner approves, or erasing the data altogether. The Commissioner exercises this power by providing a written notice, called an "enforcement notice", to the data controller or data processor. A person who receives an enforcement notice has the right to appeal it to the Circuit Court. It is an offence to fail or refuse to comply with an enforcement notice without reasonable excuse.

[11]. Section 30 of the Data Protection Acts provides that the Commissioner may bring summary proceedings for an offence under the Acts. The Commissioner also has the power to prosecute offences in relation to unsolicited marketing under S.I. 535 of 2003[44] (Electronic Communications Regulations) (as amended by SI 526 of 2008[45]). These new regulations make the sending of spam an indictable offence in Ireland for the first time. Companies that send unsolicited emails and text messages are now liable for fines of up to €250,000 or could lose 10% of their turnover[46]. Previously offenders were prosecuted in the District Court where the maximum fine was €3,000.

[12]. The required proof of intent and/or negligence for these offences appears to follow the traditional Common Law rules as applied to other offences in the jurisdiction. In section 29 of the 1988 Act, as amended, once an offence committed by a body corporate is proved to have been committed with the consent or to be attributable to the neglect of a director, manager, secretary or other officer of that body corporate that individual may also be found guilty of that offence. Any negligence on the part of the Data Controller/Processor can also be important when it comes to the civil remedies available to the victim: the data subject concerned may have remedies under the law of defamation or breach of confidentiality, but, more frequently, in negligence because in some cases a data controller or a data processor would owe a duty of care to data subjects about whom data are being kept or processed - a duty to see that damage is not caused to them by negligent handling of the data in question.

[44] Available at http://www.irishstatutebook.ie/2003/en/si/0535.html, last accessed 11.01.09.
[45] Available at http://www.attorneygeneral.ie/esi/2008/B26499.pdf, last accessed 11.01.09.
[46] Regulation 13 (9D) of Principal Regulations, as amended by Regulation 7 of SI 526 of 2008.

[13]. The Office of the Data Protection Commissioner (ODPC) received 538 complaints relating to unsolicited text messages, phone-calls and emails in 2007 compared to 264 in 2006 and 66 in 2005[47]. Tony Delaney, assistant commissioner, said the legislation was an "important new weapon" in the war on spam[48].

[14]. In 2007, the ODPC raided a number of companies that it suspected were sending unsolicited text messages. It later issued more than 300 summonses to a number of defendants. Realm Communications, run by Tom Higgins, the owner of premium-rate fortune-telling phone lines, is currently facing prosecution on 60 summonses arising from complaints made by 14 people concerning unsolicited text messages. The ODPC successfully prosecuted Clarion Marketing Limited in November 2008 for sending unsolicited text messages. The company was fined €2,000.

[15]. Under Section 12 of the Data Protection Acts 1988 & 2003, the Data Protection Commissioner is also empowered to serve an Information Notice enabling him to obtain the information requested in the Notice which is deemed necessary for the performance of his/her functions. In June 2008 Iarnród Éireann (Irish Rail) was convicted for failing to respond and supply information sought in such an Information Notice. It was the first time that the Commissioner has had to bring a prosecution against any entity for failing to respond to an Information Notice. This is indicative of the DPC's normal policy of cooperating with data controllers wherever possible, but being prepared to resort to using its full legal powers where such cooperation is not forthcoming[49].

[16]. The Data Protection Acts set out that organisations or individuals who hold personal data owe a duty of care to individual data subjects[50]. If an individual suffers damage through the mishandling of their personal information, then they may be entitled to claim compensation through the Courts and this is a matter for them and their legal advisers. The Commissioner has no function in relation to the taking of such proceedings or in the giving of legal advice.

[17]. In April 2008 it emerged that Bank of Ireland employees lost four laptops containing the details of more than 10,000 customers who obtained a quote on

[47] 2007 Annual Report, page 9, available at http://www.dataprotection.ie/documents/annualreports/AR2007En.pdf, last accessed 11.01.09.

[48] Quoted in Sunday Times article by Colin Coyle (21.12.08), available at http://www.timesonline.co.uk/tol/news/world/ireland/article5375673.ece, last accessed 11.01.09.

[49] See Press Release of the DPC, 10.06.08, available at http://www.dataprotection.ie/viewdoc.asp?Docid=744&Catid=66&StartDate=01+January+2008&m=n, last accessed 11.01.09.

[50] Section 7 of the Data Protection Act, 1988. Act No 25 of 1988, available at http://www.irishstatutebook.ie/1988/en/act/pub/0025/sec0009.html#zza25y1988s9, last accessed 08.01.09.

or took out a life insurance policy during 2007[51]. While the Financial Regulator, the National Consumer Agency and the ODPC all called on the bank to compensate the customers concerned, none of these can even compel the banks to report data protection issues, let alone levy fines for lapses in security.

[18]. On 31 October 2008 the Minister for Justice, Equality and Law Reform, Mr. Dermot Ahern, T.D., announced that he had established a new review process to examine Irish Data Protection legislation in light of concerns arising following such data breaches[52]. This process will be led by a small review group, chaired by Mr. Eddie Sullivan, and will include the Data Protection Commissioner, Mr. Billy Hawkes. The Group will be asked to examine the issues of mandatory reporting of breaches as well as possible penalties. Mr Hawkes has already made public calls for legislative changes in this regard[53].

[19]. As regards private enforcement of the DPA, the ODPC does not play a significant role in assisting individuals with their court proceedings once the Commissioner has examined any complaints and come to a decision. This is partly due to a lack of resources, but also appears part of the philosophy of the DPC to act as a kind of ombudsman and facilitator between individuals and industry players. The Commissioner encourages compliance generally, and provides detailed decisions to the parties in question, but does not regularly get involved in lengthy court battles. This results in a dearth of relevant case-law in the area, but helps the Commissioner maintain a very valuable working relationship with data controllers generally which is used to encourage an even better rate of compliance. However, there are some notable indigenous, international and European NGOs operating here with the aim of defending civil rights in the information society. These include European Digital Rights Ireland[54], Privacy International[55], Digital Rights Ireland[56] and the Irish Council for Civil Liberties[57]

[51] See article in The Sunday Tribune by Jon Ihle and Maxim Kelly, 27.04.08, available at https://www.tribune.ie/article/2008/apr/27/boi-urged-to-pay-compensation-of-40m-for-data-leak/, last accessed 11.01.09.

[52] See Department of Justice Press Release, 31.10.08, available at http://www.justice.ie/en/JELR/Pages/Minister%20Dermot%20Ahern%20announces%20Review%20Process%20to%20Examine%20Data%20Protection%20Legislation, last accessed 11/01.09.

[53] See article in The Sunday Tribune by Jon Ihle and Maxim Kelly, 27.04.08, available at https://www.tribune.ie/article/2008/apr/27/boi-urged-to-pay-compensation-of-40m-for-data-leak/, last accessed 11.01.09.

[54] See http://www.edri.org/, last accessed 12.01.09.

[55] See www.privacyinternational.org, last accessed 12.01.09.

[56] See www.digitalrights.ie, last accessed 12.01.09.

[57] See http://www.iccl.ie/, last accessed 12.01.09.

[20]. In a significant ongoing case[58] Digital Rights Ireland (DRI), a corporate body established to protect and vindicate the civil and human rights of mobile phone users in Ireland, issued proceedings in the Irish High Court to challenge the validity of aspects of Ireland's data retention legislation. According to DRI, these laws require telephone companies and internet service providers to spy on all customers, logging their movements, their telephone calls, their emails, and their internet access, and to store that information for up to three years. This information can then be accessed without any court order or other adequate safeguard and may be in breach of the European Convention on Human Rights. In July 2008 the Irish Human Rights Commission (IHRC) was granted leave to appear before the High Court as an *amicus curiae* or 'friend of the court' in the proceedings.[59]

[21]. There is significant protection given to the personal data of employees collected while applying for work as well as during and after employment. Firstly, when an employer advertises vacancies, if they do not disclose their identity initially (e.g. where applicants are asked to respond to a P.O. Box), they must do so as soon as they begin to process the application as section 2D(2)(a) requires "so far as is practicable" that the data subject be informed of the identity of the data controller. They must also disclose that it might be passed on to a third party, if that is the case.

[22]. Application forms and CVs from unsuccessful applicants need to be kept long enough to defend a potential claim of discrimination under the Employment Equality Act (i.e. twelve months), but must not be kept for longer than is necessary[60]. Records and notes of interviews will generally be accessible to both successful and unsuccessful applicants (section 4). Unsuccessful applicants, particularly those considering a discrimination claim, are likely to seek such access. Section 2(1)(c)(ii) requires that data obtained be 'adequate, relevant and not excessive'. This wording is identical to that of Art 6(1)(c) of the Directive. Employers need to ensure that any personal information, which is recorded and retained, can be justified as relevant to the selection process.

[23]. The Act does not expressly restrict an employee's right to gain access to confidential job references. Section 4(4)(a) states that an expression of opinion about a person can be disclosed to that person without the consent of the person who expressed the opinion. However, if the expression of opinion is given in confidence it seems it cannot be disclosed without such consent. This is a possible limitation in the Act on an employee's ability to access references, which have been given and received on a confidential basis.

---

[58] *Digital Rights Ireland v The Minister for Communications, Marine and Natural Resources and others.* More information available on http://www.mcgarrsolicitors.ie/category/dri/page/2/, last accessed 12.01.09.

[59] See Press Release of 1.07.08: *IHRC granted leave to appear in Data Protection Case in the High Court.* Available on http://www.ihrc.ie/home/wnarticle.asp?NID=200&T=N&Print=, accessed 08.10.08.

[60] Section 2(1)(c)(iv) DPA 1988-2003.

[24]. Employers must provide for appropriate internal security measures to ensure protection of sensitive information. The 1988 Act was silent as to the meaning of 'appropriate security measures' but the Commissioner provides some guidance as to its meaning in these situations through the publication of Case Studies, notably Case Study 3/2001[61] and the more recent Case Study 7/2008 regarding Aer Lingus[62].

[25]. In the earlier Case Study an unnamed company had created a computer file setting out performance assessment reports for individual members of staff. The file – of which staff members had been unaware – was accessible throughout the company to a wide range of line managers, including managers who had no role in relation to the staff members in question. The Commissioner held that the failure to implement appropriate access restrictions contravened the security requirements of the Act (section 2(1)(d)), and that the resulting dissemination of the file to other unauthorised staff members amounted to an incompatible disclosure of the personal data (contrary to section 2(1)(c)(ii) of the Act).

[26]. In the Case regarding Aer Lingus employees, the Commissioner received complaints that the Human Resources Division of Aer Lingus had passed on the names, staff numbers and place of employment of its staff to HSA Ireland (a healthcare organisation offering a range of health care plans) without the knowledge or consent of the employees concerned. Aer Lingus subsequently stated that they were of the opinion that this disclosure was legitimate in accordance with what it regarded as a bona fide employment purpose. The ODPC reminded Aer Lingus of its obligations under Section 2 of the Data Protection Acts with regard to the processing of personal data and it pointed out that the personal data of its staff should not have been disclosed to a third party without the consent of the employees concerned. The DPC then sought and obtained confirmation from Aer Lingus and HSA Ireland that they had destroyed the mail merge file containing the names and staff numbers had been forwarded.

[27]. The case-law underlines the practice of subsequent compliance of organisations with data protection principles following investigation by the Commissioner, suggesting an awareness that apart from the financial implications arising from conviction, businesses could also be adversely affected by the publicity generated by a prosecution (or indeed a mere complaint) by the Commissioner.

[28]. Trade unions and works councils do not appear to have played a significant role in enforcing employers' compliance with data protection legislation, directly at

[61] Available at http://www.dataprotection.ie/viewdoc.asp?Docid=123&Catid=40&StartDate=1+January+2009&m=c, last accessed 12.01.09.

[62] Available at http://www.dataprotection.ie/ViewDoc.asp?fn=/documents/casestudies/CaseStudies2007.htm&CatID=91&m=c#7, last accessed 12.01.09.

least. Major trade unions, such as SIPTU[63], do provide guidance to their members as to their rights under the relevant legislation and may be contacted by concerned individual members. There have also been situations where trade unions have cooperated with the DPC in his investigations as to whether personal data of employees was inappropriately disclosed, most notably regarding an industrial dispute at the Department of Education and Science[64] and more recently at Aer Lingus[65].

[63] See TUF Guide to Labour Law, available at http://www.siptu.ie/YourRights/TUFGuideToLabourLaw/ContractofEmployment/DataProtectionAct1988/, last accessed 12.01.09.

[64] Case Study 2 of 2000, available at http://www.dataprotection.ie/viewprint.asp?fn=/documents/caseStudies/00cs2.htm, last accessed 12.01.09.

[65] Case Study 7 of 2003, available at http://www.cosantasonrai.ie/viewdoc.asp?Docid=106&Catid=38&StartDate=01+January+2009&m=, last accessed 12.01.09.

5. Rights Awareness

[1]. A Public Awareness Survey[66] undertaken on behalf of the Office of the Data Protection Commissioner by Landsdowne Market Research in April 2008. The purpose of the Public Awareness Survey was to measure:

- the level of public awareness of data protection and privacy issues in general;
- the extent to which the public is concerned with protecting their personal information;
- the particular privacy issues of concern to them; and
- where privacy issues fall in the range of issues of concern to the public.

The questionnaire was included in the Landsdowne omnibus survey in April 2008 where a sample of 1,000 respondents aged 15+ were interviewed. This survey is designed to be representative (in terms of age, sex, social class, region and area) of the adult population aged 15 and over living in the Republic of Ireland.

[2]. One of the key findings[67] of the survey was that nearly two thirds of the population believe they have personally experienced an invasion of privacy on some level. Over one third of respondents have received unsolicited text messages from commercial organisations, with the highest incidence being among under 35's (45%) and respondents in Dublin (47%).

[3]. Not surprisingly, of the issues put before respondents a good health service (89%) and crime prevention (87%) were seen as the most important issues affecting them. This was followed by privacy of personal information with 84% of those surveyed indicating that privacy of personal information was very important to them.

[4]. Meanwhile, almost one in five respondents believe that there is not appropriate access controls in place in both public sector and private sector organisations to prevent employees from accessing personal information inappropriately. Medical records, financial history and credit card details attach the highest levels of importance in terms of keeping this information private, with over 8 out of 10 respondents attributing a 'very important' rating to these issues.

[66] Full survey available at http://www.dataprotection.ie/docs/Public_Awareness_Survey_2008/794.htm, last accessed 10.01.09.

[67] Report presenting the findings of survey available at http://www.dataprotection.ie/docs/Public_Awareness_Survey_2008_Report/821.htm, last accessed 10.01.09.

[5]. Encouragingly, prompted awareness of the Data Protection Commissioner continues to increase, with 58% of respondents aware of the Data Protection Commissioner. This has continued to increase significantly since 1997 when only 25% of people surveyed were aware of the Data Protection Commissioner. It found that over 70% of respondents were aware of their right to: have their name removed from junk mail lists; have their telephone number removed from direct marketing lists; have inaccurate information about them corrected or deleted; and get a copy of information about them held by any organisation.

[6]. However, 21% of respondents believed that they had no right to have 'any' of their medical records deleted, while over one in five respondents (22%) believed they had the right to get personal information about other people. In his reaction to the results of the survey the Commissioner noted the increasing levels of importance attached by Irish people to the privacy of their personal details, and stated that the results of the survey would be used to shape the future work of his Office[68].

[68] Press Release of 12.08.08, available at http://www.dataprotection.ie/viewdoc.asp?DocID=815, last accessed 10.01.09.

6. Analysis of deficiencies

[7]. One of the main deficiencies in the Irish system of data protection is the lack of a concrete requirement for all Government Departments to consult with the Office of the Data Protection Commissioner when drafting legislation which may or may not impact on privacy and data protection issues. While, as outlined above, the DPC has been consulted on some high profile pieces of legislation in recent times, the current Commissioner continues to describe the level of consultation by the Department of Justice, Equality and Law Reform in particular as "patchy"[69]. This lack of consultation is a problem faced by other members of the so-called 'justice family' in Ireland, most notably by the Irish Human Rights Commission. While the DPC continues to try to foster good working relationships with individual Government Departments, he fears that consultation with his Office is beginning to be seen as an extra barrier to be overcome by legislators, rather than as a contributing factor to effective legislation[70].

[8]. Another key deficiency in the Irish data protection system would appear to be the lack of a legal obligation for data controllers/processors to report data breaches either to the Gardai or directly to the Commissioner. This deficiency was highlighted during this year when media sources disclosed the details of a serious data breach at Bank of Ireland, one of the largest financial institutions in the State[71]. While, as outlined above, the Minister of Justice has formed a high-level working group of experts including the current Commissioner to investigate whether legislative changes are required in this regard, there has been no progress on this issue as of yet.

[9]. The current system of voluntary reporting fits in with the general theme of the DPC as a body designed to help and ensure compliance, rather than one focused on punishing breaches (with the notable exception of its powers under the 2008 Electronic communications Regulations). It follows that this voluntary reporting system would lose all effectiveness if organisations feared fines or awards of damages against them as a result of an adverse decision of the DPC in their regard. Thus, the Commissioner appears satisfied that the current system actually encourages good working relationships with data controllers generally, and therefore the lack of compulsory breach-reporting requirement does not overly impact on the data protections guaranteed to the population. However,

[69] Interview with author, 09.01.09.
[70] 2007 Annual Report, page 22, available at http://www.dataprotection.ie/documents/annualreports/AR2007En.pdf, last accessed 09.01.09.
[71] See article in The Sunday Tribune by Jon Ihle and Maxim Kelly, 27.04.08, available at https://www.tribune.ie/article/2008/apr/27/boi-urged-to-pay-compensation-of-40m-for-data-leak/, last accessed 11.01.09.

the ODPC is said to be closely monitoring the situation in the UK where their counterparts, the Information Commissioner's Office[72], appear to take a more aggressive stance at the risk of losing the kind of cooperation the ODPC have come to expect from data controllers here.

[10]. The DPA, like Directive 95/46, has an extremely broad application and applies to many, if not quite every, processing operation which can be undertaken with regard to personal data. The DPA contains a variety of exemptions, with some categories of information being exempt from the entirety of the Acts and others only being exempt from certain provisions such as the right of access.

[11]. The most notable exemptions from the entirety of the DPA are: personal data that in the opinion of the Minister or the Minister for Defence is kept for the purpose of safeguarding the security of the State; personal data that the controller is required by law to make available to the public; and personal data kept by an individual and concerned only with the management of his/her personal, family or household affairs or kept by an individual only for recreational purposes[73].

[12]. Section 5 of the Act sets out a number of restrictions on the right of access guaranteed under Section 4. Firstly, data kept for the purpose of preventing, detecting or investigating offences is not covered[74]. Another notable category of information exempted is data processed for the maintenance of good order and discipline in prisons[75]. Possibly the broadest exemption refuses a right of access where such would be contrary to the interests of protecting the international relations of the State[76].

[13]. It is the widely held view of commentators in this area that deliberate legislative changes will be required to repair the major deficiencies in the current system pointed out above. As also mentioned above, a high level committee has been formed to discuss possible improvements to the current legislation, especially as regards a proposed legal compulsion on Irish data controllers to report all breaches to the DPC. As regards the lack of consultation between Government departments and the Commissioner, it is doubtful that the attitude of legislating departments towards the DPC will ever change voluntarily, so a legislative requirement to seek the Commissioner's approval may well be required. This would likely be seen as adding an extra hurdle to the already lengthy legislative process, and so would probably run into considerable opposition amongst the State's law-makers. At the current point in time it would not appear that the political will is present to force such a move through. An alternative would, of

[72] See http://www.ico.gov.uk/
[73] Section 1(4) of DPA 1988-2003
[74] Section 5 (1)(b) of DPA 1988-2003
[75] Section 5 (1)(c) of DPA 1988-2003
[76] Section 5 (1)(e).

course, be to increase the training and privacy rights-awareness of the law-makers themselves in the hope that this would encourage greater consultation and cooperation with the Commissioner in the future.

7. Good Practice

[1]. Whereas under the 1988 Act the Commissioner only had the power to approve codes drawn up by trade associations, the 2003 Act gives the Commissioner the power to propose and prepare codes, which if approved by the *Oireachtas* (Parliament) will have binding legal effect[77]. The Commissioner is of the opinion that codes of this nature benefit everybody. The Data Protection Acts provide for the preparation of sector-specific codes of practice to allow for a better understanding of the requirements of the Acts. The Directive's encouragement to produce such codes is taken as a recognition that the statutory data protection requirements can sometimes benefit from elaboration when they are applied within particular sectors.

[2]. A code that is well researched, written and reflective of the processing of personal data that takes place in a sector is of enormous benefit according to the most recent Annual Report of the Commissioner[78]. For the particular sector involved, it applies the obligations contained in the Acts to the particular circumstances within that sector. This clarifies the standards expected and serves as a useful template for consistent training of all persons handling personal data in the sector. The sector can also benefit from the increased public and media focus on data protection standards. It is hoped that an increasingly discerning public will display a preference for organisations that have publicly committed themselves to high standards of data protection.

[3]. 2007 marked a key year in the development of codes of practice by the Office of the DPC. They worked with An Garda Síochána, the Personal Injuries Assessment Board (PIAB), and the recruitment and insurance sectors via appropriate representative bodies. All of these sectors were singled out as areas where clarification and transparency in terms of personal data and confidentiality would be beneficial. The data protection code of practice for An Garda Síochána, launched in November 2007, was the first code of practice to be formally approved by a Data Protection Commissioner under the provisions of the Acts.

Elsewhere, the Commissioner himself has publicly welcomed the trend towards voluntary disclosure of data breaches as an example of good practice[79]. It allows his Office to reassure members of the public that they are aware of a particular

[77] Section 13, DPA 1988-2003

[78] 2007 Annual Report, page 17, available at http://www.dataprotection.ie/documents/annualreports/AR2007En.pdf, last accessed 12.01.09.

[79] 2007 Annual Report, page 16, available at http://www.dataprotection.ie/documents/annualreports/AR2007En.pdf, last accessed 12.01.09.

problem and that the organisation in question is taking the issue seriously. It also allows the ODPC to advise the organisation, at an early stage, how best to deal with the aftermath of a disclosure and how to ensure that there is no repetition. It is hoped that the development of best practice in this area is being observed by other sectors - including the public service. The ODPC were notified of eleven separate cases of accidental disclosure in the course of 2007 involving data controllers in the financial services, insurance, charity and medical services sectors. Some of these disclosures included information related to thousands of individuals or information of particular sensitivity. Of course, the practice of informing the Office and customers of a disclosure is not seen as a substitute for the proper design of systems to secure customer and employee data from accidental or deliberate disclosure to third parties.

8. Annexes

Annex 1 - Tables and Statistics

Please complete the table below

	2000	2001	2002	2003	2004	2005	2006	2007
Budget of data protection authority	€432,454	€524,874	€750,173	€1,132,733	€1,323,676	€1,392,782	€1,281,521	€1,835,375
Staff of data protection authority	7	14	16	18	21	22	22	22
Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative	n/a[80]	n/a	n/a	n/a	n/a	n/a	n/a	n/a

[80] The Office of the Data Protection Commissioner does not release such information, and is not subject to Irish Freedom of Information legislation. For illustrative examples of such procedures please refer to individual annual reports, available at http://www.dataprotection.ie/ViewDoc.asp?DocId=-1&CatID=50&m=p, last accessed 29.01.09.

Number of data protection registrations	2,880	3,099	3,632	4,618	5,509	5,933	6,380	5,699
Number of data protection approval procedures	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Number of complaints received by data protection authority	131	233	189	258	385	300	658	1,037
Number of complaints upheld by data protection authority	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Follow up activities of data protection authority, once problems were established (please disaggregate according to type of follow up activity: settlement, warning issued, opinion issued, sanction issued etc.)	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a

Sanctions and/or compensation payments in data protection cases (please disaggregate between court, data protection authority, other authorities or tribunals etc.) in your country (if possible, please disaggregate between sectors of society and economy)	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a

Any other tables or statistics relevant for assessment of effectiveness of data protection, where available

Annex 2 – Case Law

Please present at least 5 cases on data protection from courts, tribunals, data protection authorities etc. (criteria of choice: publicity, citation in media, citation in commentaries and legal literature, important sanctions) in your country, if available (please state it clearly, if less than 5 cases are available)

Case title	McGee v. Attorney General and Revenue Commissioners
Decision date	8/9.06.72 and 6/7/8/9.11.73
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	[1975] 109 I.T.L.R. 29. Irish Supreme Court
Key facts of the case (max. 500 chars)	Plaintiffs attempted to illegally import contraceptives into the State for their own personal use. The case revolved around the legality of such prohibitions in light of the Irish Constitution's indirect privacy guarantees.
Main reasoning/argumentation (max. 500 chars)	The plaintiffs argued that the legislation in question was unconstitutional because it did not defend or vindicate their personal rights – most notably the right to privacy in their private and marital lives.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The approach taken by the court indicated that justice is to be placed above the law, and that fundamental human rights are recognised – not created – by the Constitution. It was also confirmed that individuals have natural and human rights over which the state has no authority and, further, that the family as the natural primary and fundamental unit group of society has rights as such which the State cannot control.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	This decision saw the beginning of the development of 'natural law' as a basis for fundamental human rights, especially the right to privacy and freedom from excessive State interference in private lives of individuals.
Proposal of key words for data base	McGee, privacy, natural law, fundamental rights

Case title	Geraldine Kennedy, Bruce Arnold and Mavis Arnold v Ireland and the Attorney General
Decision date	12.01.87
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	[1988] I.L.R.M. 472 Irish High Court
Key facts of the case (max. 500 chars)	On 14 May 1982, the then Minister of Justice issued warrants authorising the communication to the Garda Assistant Commissioner of all conversations taking place on the private telephones of the plaintiffs. The plaintiffs claimed that such warrants and the telephone *'tapping'* which ensued were in breach of their Constitutional rights. The State conceded at the hearing that there was no justification for the tapping of the plaintiff's telephones.
Main reasoning/argumentation (max. 500 chars)	The plaintiffs argued that they were guaranteed a right to privacy under the Irish Constitution because it flows from the nature of the society and State that the Constitution creates. They also argued that the State are under an obligation to respect and vindicate all individuals' rights to privacy and a private life.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The court recognised that the right to privacy is one of the fundamental personal rights of the citizen which flow from the Christian and democratic nature of the State. It may, however, be restricted by the Constitutional rights of others and by the requirements of the common good. The nature of the right to privacy is such that it must be ensured to guarantee the dignity and freedom of the individual in a democratic society.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The court held that the State had failed: (a) to defend and vindicate the plaintiffs' personal rights, (b) to respect the privacy of the plaintiffs in the exercise of their profession as political journalists and in the living of their private lives by not interfering with listening to and tapping their telephone conversations, and (c) to respect the guarantee to all citizens to express freely their convictions and opinions. The plaintiffs were awarded £50.000 in total damages
Proposal of key words for data base	Privacy, fundamental rights. Journalistic freedoms.

Case title	P J Madigan and P Madigan v The Attorney General, The Revenue Commissioners and Others
Decision date	20.11.84
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	[1983] T.I.T.R. 127. Irish Supreme Court
Key facts of the case (max. 500 chars)	The plaintiffs challenged the constitutionality of taxation legislation, whereby exemption or relief from tax could only be obtained, in many cases, by requiring a full disclosure to the assessable person of the income of all "relevant persons" living with him. It was argued that this was an unwarranted invasion of the right of privacy which such persons were entitled to enjoy in relation to their own affairs.
Main reasoning/argumentation (max. 500 chars)	The plaintiffs claimed that the legislation failed to respect their right to equality before the law, represented an unjust attack on their rights of property, in contravention of the provisions of *Article 40.3* and contravened the right of privacy which, they claimed, was one of the undefined rights protected by that Article. The defendants maintained, however, that it had never been considered that such right to privacy as might be held to exist under the Constitution, extended to the financial affairs of a member of a family.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The right to privacy guaranteed by the Constitution was described as being subject to the State's right to maintain public order in the common good. It was held that the legislation did not purport to authorise any invasion of the privacy of such members of the household. Even if there were a statutory provision compelling disclosure of information about income where this information was relevant to determine the tax liability of another person, the court seemed doubtful that any constitutional guarantee would be thereby infringed.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The claims of the plaintiffs were not sustained.
Proposal of key words for data base	Privacy rights subject to the common good

Case title	Realm Communications v. Data Protection Commissioner
Decision date	09.01.09
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	[2009] IEHC 1, Irish High Court, judgement by Mr Justice McCarthy
Key facts of the case (max. 500 chars)	The Data Protection Commissioner had begun proceedings to prosecute Realm Communications for 300 violations of anti-spam legislation. Realm Communications sought relief against these prosecutions by arguing that the Commissioner was obliged under its own founding statue to set aside time for attempting to reach an amicable solution to such issues – something which was not done in this case.
Main reasoning/argumentation (max. 500 chars)	The applicant argued that the Commissioner can only lawfully exercise his power under the Acts to summarily prosecute on foot of complaints of contraventions if the rest of the Acts have been complied with. Essentially, Realm claimed that it is a condition precedent to a prosecution in respect of the offences that an attempt be made to seek amicable resolution of the complaints giving rise to the charges
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The court held that neither the Acts in question nor the underlying EC Directives set out an attempted amicable solution as a condition precedent for a prosecution. The court also recognised the Commissioner's right to attempt to find an amicable solution in tandem with the preparation of, and the ultimate commencement of, criminal proceedings.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The court refused the reliefs sought, and the DPC's right to by-pass the amicable solution stage of proceedings where appropriate was confirmed.
Proposal of key words for data base	Enforcement of data privacy legislation, Amicable solutions

Case title	Haughey and Others v Attorney General and Others
Decision date	28 July 1998
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	[1998] T.I.T.R. 67, Irish Supreme Court, judgement by Mr Chief Justice Hamilton
Key facts of the case (max. 500 chars)	This appeal to the Supreme Court from the decision of the High Court challenged practically every aspect of the McCracken Tribunal (part of a series of inquiries into payments to politicians in Ireland) and the constitutionality of the *Tribunal of Inquiry (Evidence) Act 1921*. This inquiry related to the investigation and findings of the Tribunal in regard to the payments in excess of £1 million made by (businessman) Ben Dunne to (former Taoiseach) Charles Haughey. The judgment recognised the constitutional right to privacy, and went on to discuss the extent of that right.
Main reasoning/argumentation (max. 500 chars)	It was submitted on behalf of the plaintiffs/appellants that the terms of the investigations conducted by the Tribunal of Inquiry violated their constitutional right to privacy – most notable the privacy of their financial records and banking transactions. They argued that the protection granted to them indirectly by the Irish Constitution was near-absolute, and that the State Parliament had no right to breach their right to privacy in order to conduct an inquiry.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The Court accepted that the constitutional right to privacy extends to the privacy and confidentiality of a citizen's banking records and transactions. However, it also held that the exigencies of the common good may outweigh this constitutional right. The encroachments on such rights were justified in this particular case by the exigencies of the common good but any such encroachments must however be only to the extent necessary for the proper conduct of the inquiry.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	Relief was refused on these particular points because the Court recognised that the common good requires that matters considered by both Houses of the Oireachtas to be of urgent public importance be enquired into.
Proposal of key words for data base	Privacy, bank records, common good.

[4]. AUTHOR'S NOTE: TEXT OF ORIGINAL JUDGEMENTS ATTACHED IN A SEPARATE DOCUMENT AS REQUESTED