THE APPLICATION OF DATA PROTECTION LAW TO THE EMPLOYMENT SECTOR

By Gemma Neylon

Employment relationships involve the supply and collection of personal information, including sensitive personal information. This process includes the collection of information for the purposes of recruitment, paying wages, deducting taxes and union dues, complying with health and safety laws, and assessing performance. Some practices, such as the monitoring of employee's Internet and email access, highlight controversial issues of privacy[1].

Data protection legislation, the Data Protection Act 1988 as amended by the Data Protection Act (Amendment) 2003 (which incorporated the 1995 Data Protection Directive 95/46/EC), supplements the common law in this area and places more formal obligations on employer organisations about how they handle employee information[2]. This essay will consider privacy issues and practical data protection issues that often arise in employment situations, with particular focus on issues arising from recruitment and employee monitoring.

Relevant Legislation

The 2003 Data Protection (Amendment) Act has updated the 1988 Act to fully implement the provisions of the 1995 Directive, the basic principles of which had already been introduced. The main changes, which the 1995 Directive has brought about, are:

- Extending the application of the rules to paper files;
- Requiring consent to process personal information;
- Extending the registration requirements of data processors and controllers;

---

*This essay was awarded the Conway Kelliher Tobin prize 2005.

[1] A&L Goodbody, *A Practical Guide to Data protection Law in Ireland*, (Round Hall Press, 2003) Chap. 5 For a general overview of the application of data protection law to the employment sector

[2] *Ibid*

- Regulating the transfer of information outside the EEA;
- Extending the powers of the Commissioner to monitor compliance.
-
-

Recruitment and Selection

Many data protection issues arise in relation to recruitment and selection. There is a need for awareness of data protection obligations, due in part to the obligations imposed on employers on other fronts by the increasing volume of employer legislation, including the Employment Equality Act 1998. Employees or unions can use data protection access rights in order to gather information designed to support a claim under this and other legislation.

Advertising

When an employer advertises vacancies, if he or she does not disclose her identity initially (e.g. where applicants are asked to respond to a P.O. Box), she should do so as soon as she begins 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 should also disclose that it might be passed on to a third party, if that is the case.

Applicants and CVs

Employers need to take into account the fact that the application form should say to whom the information is going and should set out the fact that it will be used in a way other than would be expected, if that is the case. They may need sensitive personal information from potential applicants, for example, details of criminal convictions or health problems. A&L Goodbody point out that it may not be appropriate to ask the same questions of all prospective employees. For instance, details of offences involving fraud or dishonesty may be relevant for a sensitive or senior position involving the handling of money in a bank, but may not be relevant for the recruitment of a bank receptionist.

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 (section 2(1)(c)(iv)).

Interviews

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.

Selection

Section 6B prohibits decision-making based solely on automated processing, with some exemptions, such as where the decision is taken while entering a contract at the request of the data subject. This is an exemption of potential relevance in the context of entering into an employment contract. The Director of the Personnel Policy Research Unit for the UK Information Commissioner suggests that rather than attempting to prove that a decision is not based "solely" on processing by automated

means, employers should legitimise a decision based on automated processing on the grounds that it was taken with a view to entering into a contract with the individual[3].

References

Unlike its UK equivalent, 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 (e.g. references which have been *stated* to be given on the understanding that they will be confidential).

Data Protection Access Requests

It is illegal for an employer to require the employee to make such a request to another party or to provide information obtained through a request from another party (section 4(13)). However this provision will not come into force until 2007, due to the fact that there is no official method of vetting employees in Ireland.

Case Study: 3/01

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 this case. A 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. Following a complaint by the employees concerned to the Commissioner, the company explained that the 'access permissions' on this file had inadvertently been set to allow numerous people outside of his management team to read it. The Commissioner confirmed that the failure to implement appropriate access

[3] Chater, "*The Uses and Misuses of Personal Data in Employer / employee Relationships*" (2003), from www.dataprotection.gov.uk/dpr/dpdoc.nsf

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). However, the Company had taken immediate steps to address the issues in terms of ensuring that appropriate security measures are in place and improving awareness of staff and management regarding the importance of adhering to correct procedures. Section 2(c) of the 2003 Act (which implements Art 17 of the Directive) now gives more detailed guidance on the determination of appropriate security measures.

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.

Obtaining and Holding Personal Information on Employees

Employers who keep personal data about their employees are, in common with all data controllers, bound by the provisions of section 2 of the Data Protection Act which requires *inter alia* that personal data: (i) be obtained and processed fairly (section 2(1)(a)); (ii) be kept only for one or more specified and lawful purpose (section 2(1)(c)(i)); and (iii) be adequate, relevant and not excessive in relation to the specified purpose or purposes (section 2(c)(iii)). Employees should be told what information you hold about them, how it will be used, to whom it will be disclosed and of their right to access the information (section 2(d)). Employees have the right to object to the processing of their personal data under section 6(a). However the requirement of proving *substantial* damage or distress greatly limits the grounds on which employees could object.

Monitoring and Surveillance at Work

A number of the requirements of the Data Protection Act will come into play whenever an employer wishes to monitor employees. The Act does not prevent an employer from doing so, but such monitoring, where it goes beyond one individual simply watching another and involves the manual recording or automated processing of personal information, must be done in a way which complies with the Act[4]. Monitoring and surveillance of employees is a controversial issue. The American Civil Liberties Union conveys the extremity of the U.S. situation thus: '[t] he computer's eye is unblinking and ever-present. Human workers are being tracked like machines by machines'[5].

Orla Ward suggests that in the twenty-first century employee surveillance will be one of the major areas of conflict between employee and employer[6]. As far back as 1999, the Irish Times reported that a trade union leader had called upon employers to curtail electronic surveillance of employees in the workplace[7]. The problem has since become widespread, with two Dublin companies announcing plans in January 2004 to introduce powerful computer systems capable of monitoring all staff telephone and internet use[8].

In 1977, a report of the Privacy Protection Study Commission of the U.S. Electronic Privacy Information Commissioner (EPIC), focussed on the creation, maintenance, use and disclosure of employee records[9]. These same issues remain of increasing concern today. However, advancing technology has further complicated the issue. Technology has increased the risks to an employer of misuse of email and Internet by employees. On the other hand the likelihood of intrusion into private communications or activities are increased.

---

[4] U.K. Information Commissioner Employment Practices Data Protection Code: Part 3: Monitoring at Work, section 2, available at http://www.informationcommissioner.gov.uk/ (last visited 5/3/05)
[5] American Civil Liberties Union, Legislative Briefing Kit on Electronic Monitoring, March 2002, available at www.aclu.org (last visited 5/3/05)
[6] Ward, "Is Big Browser Watching You?" (2000) 150 *NLJ* 1414
[7] Yeates, "Union calls on employers to curtail surveillance", The Irish Times, Aug 28, 1999
[8] "Company to monitor staff and Internet use", The Irish Times, Jan 23 2004
[9] The Privacy Protection Study Commission, "Personal Privacy in an Information Society" (1977) Chap. 6, available at www.epic.org/privacy/ppsc1977report/c6.htm (last visited 5/3/05)

According to a study in 2000 by the American Management Association, more than seventy three percent of companies monitor employees' Internet use[10]. However, other figures can be used to shed light on the reasons for this. A recent survey by internet security company Entropy found that seventy two percent of pornographic sites are viewed during working hours and that an employee spends two hundred and twenty hours a year surfing the net[11]. In a 1997 report the UN estimated that a staggering ninety percent of economic computer crime is committed by employees[12]. Monitoring can be justified on the ground of crime detection: retailers in the U.S. for example, lose an average of 1.7 percent of their revenue – about $40 billion a year in cash and inventory – to unexplained losses, almost 45 percent of which results from employee theft[13]. On the other hand, studies have shown that surveillance takes its toll on employees in terms of stress, morale, apprehension, motivation and trust, all of which lead to increased absenteeism, turnover and lower productivity. In any case, whether the benefits of employee monitoring outweigh its undesirable effects or vice versa, issues relating to data protection and privacy arise in all circumstances in which employee monitoring is undertaken.

The Ontario Information and Privacy Commissioner in 2001 illustrated the tension between employees' right to privacy and the need to protect employers' legitimate business interests: "[p] privacy is not an absolute right, and in the workplace, is balanced against the employer's legitimate interest in maintaining a safe, efficient and productive workplace. That is not to say that the employee's privacy rights must give way completely to the concerns of the employer – the employer should seek to ensure that its policies and practices as far as possible give effect to both the employer's needs and the employee's privacy."[14]

In May 2002, the Article 29 Data Protection Working Party published its report on the issue of monitoring and surveillance of electronic communications in the workplace.

---

[10] Wofford, R. & Wynne, J., "*Negotiating the Workplace privacy Minefield*" (2001) available at www.workforce.com (last visited 5/3/05)
[11] *Supra,* n. 6, p.2
[12] *Ibid*
[13] "More Stores now Spy on Employees", The New York Times, July 11 2001 available at www.aclu.org?Privacy/Privacy.cfm (last visited 5/3/05)
[14] O'Donoghue, M. "Reasonableness in the Context of Workplace Privacy" (2001), available at www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=11559&N_ID=1&pt (last visited 5/3/05)

It stated that balancing the different interests at stake involves the principle of proportionality.

> "It should be clear that the simple fact that a monitoring activity or surveillance is considered convenient to serve the employer's interest would not solely justify and intrusion in worker's privacy"[15].

As normal data protection principles apply, monitoring and surveillance will generally require the consent of individual employees (section 2A) or need to be permitted on one of the other grounds in section 8 on which processing are permitted, for example, that the monitoring is necessary to prevent or detect a crime (section 8(b)). Monitoring generally needs to be undertaken for a specified and legitimate purpose, which has been made clear to the employees (section 2(1)(c)(i)) (7).

Employers need to bear in mind certain practical implications of the data protection principles. For example, if the stated purpose of monitoring internet access is to ensure the integrity of the firm's computer systems, using it for the purpose of disciplining an employee for excessive use of the internet may be incompatible with that stated purpose (contrary to section 2(1)(c)(ii))[16]. The employer should provide information through a policy, disclosing what monitoring should take place and why (section 2D(1)(a)). Employees have a right to access personal information collected by monitoring and surveillance in the same way as they have a right to access any other kind of personal information. However, section 2(4) of the 2003 Act specifically excludes a right to access any back-up data.

Monitoring should be designed to prevent rather than to detect misuse. For example, it is preferable, for data protection requirements, to block access to inappropriate Internet sites by using web filtering software rather than monitoring on an ongoing basis. Furthermore, employers should target monitoring at areas of highest risk rather than in all areas of the business. As A&L Goodbody point out, if they can show a considered analysis of a risk before monitoring, the Commissioner is more likely to accept its reasonableness[17].

---

[15] Available at http://europa.eu.int?comm/internal_market/privacy/docs/wdocs/2002/wp55 (last visited 5/3/05)
[16] *Supra* n.1, p. 62
[17] *Supra* n.1, p. 63

Data Protection Commissioner's Report 1999: Data Protection in the Workplace

Part three of the Data Protection Commissioner's Annual Report 1999 addresses the issue of employee monitoring. This is identified as 'an area of growing importance to both employees and employers and their representative bodies'. Much will depend on the culture of the particular employment in question. As Galkin remarks, 'much of the law of privacy in the workplace turns on the reasonable expectation of privacy'[18]. If employees have been using the company email system for personal correspondence, with the tacit agreement of the employer, then 'it is most unlikely that an employer may access those personal items of correspondence without contravening the Data Protection Act'. Section 2(1)(a) of the Act requires that personal data be *'obtained and processed fairly'*. Therefore such emails should not be accessed without the express permission of the employees concerned[19].

The Situation in other EU Member States

It is rare for countries to have introduced specific legislation applying data protection rules to the employment context – this has occurred most notably in France, Finland, Greece (in the form of a Data Protection Authority directive) and, to some extent, Portugal.

Given the general paucity of specific legislation on employees' privacy at the workplace, the introduction of provisions has been discussed or proposed in a number of countries. In Finland, a working party (including social partner representatives) established by the Ministry of Labour at the behest of Parliament, has examined certain specific issues not addressed by their Act on Data Protection in Working Life (2001). It issued its report in June 2003 (F103072031f) proposing new legislation defining and limiting employers' rights to use drug tests and video surveillance and to read employees' emails. In Germany an Employee Data Protection Act

[18] Galkin, "The Computer Law Report", (December 28th 1995), available at http://www.eff.org/Privacy/Workplace/galkin_workpriv_122895.article (last visited 5/3/05)
[19] Data Protection Commissioner Annual Report 1999, part 3: Particular Issues: Data Protection in the Workplace, p.33, available at www.dataprivacy.ie/6e.htm (last visited 5/3/05)

(Arbeitnehmerdatenschutzgesetz) has been discussed for some years, and the coalition of the current 'red-green' government provides for the introduction of such a law[20].

Despite these promising steps, the general absence of specific legislation on data protection remains. As a result a number of national supervisory bodies have issued detailed codes of practice on employee monitoring at workplace, including Denmark, Greece, Portugal and the United Kingdom. We will now look briefly to that of the U.K. for guidance.

The Information Commissioner's Employment Practices Data Protection Code: Part 3: Monitoring at Work

The Code, issued in June 2003, contains a lengthy section on workplace surveillance, since 'a number of the requirements of the Data Protection Act will come into play whenever an employer wishes to monitor employees'. It seeks to clarify the application of the law and to protect employees from unfair or excessive information gathering. The general position adopted by the Information Commissioner is that employers should be open about the use of monitoring which should, further, be designed to intrude as little as possible on employees' privacy and on their 'autonomy': the "right to expect a degree of trust from his/her employer, and be given reasonable freedom to determine his/her own actions without constantly being watched or asked to explain must also be respected". It emphasises the need for proportionality between any intrusion on privacy and 'the benefits of the monitoring to a reasonable employer'. As Oliver suggests, proportionality is perhaps the *only* appropriate way to reconcile employee privacy with employers' interests[21].

The supplementary guidance to the code provides a number of useful examples of the application of data protection law to everyday activities. For example, it reminds employers that the monitoring of telephone calls will often also involve collecting information about people who make calls to the organisation. Where this involves the processing of personal data, these people should also be informed of the monitoring

[20] Delbar., Mormont & Schots, "New Technology and Respect for Privacy in the Workplace" (2003) *European Industrial Relations Observatory Online*.
http://www.eiro.eurofound.ie/2003/07/study/tn0307101s.html
[21] Oliver, "Email and Internet Monitoring in the Workplace: Information Privacy and Opting-Out" (2004) *ILJ*

and the reasons for its being carried out. This may be done through the use of recorded messages on telephone systems.

The code suggests that the data protection principles require that:[22]

- monitoring is used only for identified 'specific business purposes';
- employees are given the opportunity to challenge and explain information gained through monitoring if it is to be used 'in a way that might have an adverse impact' on them. (For example, it must be remembered that websites can be visited unwittingly through unintended responses of search keys, unclear hypertext links, misleading banner advertising or mis-keying[23]).

The EU Commission, according to its June 2003 mid-term review of the social policy agenda, is planning a draft Directive on the application of data protection law to the employment environment in 2004 or 2005. The proposals include a national prior check by a national data protection supervisory authority of any system of surveillance and a prohibition on routine monitoring of each individual worker's email or internet use[24]. It proposes further that employee consent should not be relied upon to legitimise the processing of personal data because of the difficulties in ensuring it is genuine free consent, given the inherent power imbalance in the employment relationship.

Thus we see that at EU level the issue is high on the agenda from a legislative point of view. At International level the ILO has drawn up a Code of Practice on the protection of workers' personal data, while a global trade union body, UNI, has issued a Code of Practice on online rights at work[25].

Simitis has re-iterated the need for a Regulation on the protection of employees' data[26]. He envisages building on the comparative experience of the Member States, to reflect both the reality of the modern employment relationship and a new normative

[22] Collins, Ewing, and McColgan, *Labour Law: Text and Materials* (Hart Publishing 2001), p. 683
[23] U.K. Information Commissioner Employment Practices Data Protection Code, Part 3: Supplementary Guidance, section 3.3.12
[24] *Supra* n.20
[25] *Ibid*
[26] Simitis, "Reconsidering the Premises of Labour Law: Prolegomena to an EU Regulation on the Protection of Employees' Personal Data" (2004) 5 *ELR* Vol. 5. No. 1. March 1999. p. 45-62

vision of the workplace, which aims to inject such relationships with a measure of communicative participation.

The Situation in the U.S. and Canada

Several U.S. groups are actively involved in workplace monitoring issues. The National Work Rights Institute, Workplace Fairness, and the American Civil Liberties Union, to name a few, advocate stronger government regulation of employee monitoring[27]. In Canada, the Privacy Commissioner and the Ontario Information and Privacy Commissioner remain committed advocates of regulatory changes respecting workplace privacy issues. In 1992 public opinion surveys in Canada consistently revealed that a majority of those questioned were concerned with what they perceived to be an erosion of personal privacy[28]. The Ontario Commissioner states that 'the goal of effective regulatory changes which are satisfactory for both employees and employers is essential and achievable'[29]. It is precisely this balance that the forthcoming EU Directive will seek to achieve.

Conclusion

Mc Donagh, albeit in a different context, states that access to information is regarded increasingly as a fundamental requirement of the European democratic framework[30]. Access to personal information undoubtedly comes within this fundamental requirement. Hockey and Smith are correct in remarking that over the last three

[27] Utility Consumers' Action Network/Privacy Rights Clearinghouse, "Employee Monitoring: Is there Privacy in the Workplace?" Sept 2002, available at www.privacyrights.org/fs/fs7
[28] Information and privacy Commissioner, Ontario, "Workplace Privacy: A Consultation Paper" June 1992, available at www.ipc.on.ca/scripts
[29] Information and Privacy Commissioner, Ontario, "Workplace Privacy: The Need for a Safety Net" Nov 1993, available at www.ipc.on.ca/scripts
[30] Mc Donagh, "The Interaction of European Community and National Access to Information Laws: An Irish Perspective" (2000) 9 *IJEL* 216-236

years, the growth of the Internet and email has kept the subject of employees' rights vs. corporate security under an increasingly political, media and legal spotlight[31].

Ward, on the other hand, is surely erring in stating that '[t] he fact is, however stringent the law, if an employer wishes to infringe an employee's privacy illegally, there are many methods of so doing without being detected'. On the contrary, the Data Protection Act confers many significant safeguards on employee privacy. Nonetheless, it does *specifically* address employment sector issues.

This essay has attempted to address issues arising from the application of data protection law to the employment sector. The public policy agenda on privacy issues, and thus on data protection, is ever evolving. Intervention to control the workplace respecting electronic monitoring, employee testing, and the misuse of employment records are a critically important public policy goal internationally. With this in mind we can look forward to the EU Directive on data protection in the workplace specifically addressing the issues addressed above. Until then, the current Data Protection Act, being an omnibus piece of legislation, does leave workers in particular sectors uncertain as to the application of data protection to their activity. The employment sector is a prime example.

[31] Hockey & Smith, "Cyberliability – Oh what a Tangled Web we Weave", (2002) 7 *CFS* pp. 5-7 available at http://www.ingentaconnect.com/content/els/13613723/2002/00002002/00000007 (last visited 5/3/05)

Bibliography

- Compendium of Data Protection Acts 1988 and 2003
- Council Directive on the Protection of Individuals With Regard to the Processing of Personal Information (Directive 95/46/EC)
- Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981)
- OECD Guidelines governing the protection of privacy of transborder flows of personal data (1980)
- A&L Goodbody *A Practical Guice to Data Protection Law in Ireland,* 2003, Round Hall Press.
- Clarke *Data Protection Law in Ireland* Round Hall Press, 1990.
- Collins, Ewing & McColgan *Labour Law: Text and Materials* Hart Publishing, 2001.
- Kelleher & Murray *Information Technology Law in Ireland,* Butterworths, 1997.
- Reed & Angel (Eds.) *Computer Law* 2000, 4th Ed, Blackstone Press.
- Forde *Employment Law* 2001 2nd Ed, Round Hall Press.
- http://www.lexisnexis.com/professional
- Data Protection Commissioner: http://www.dataprivacy.ie/
- Electronic Privacy Information Centre: http://www.epic.org/
- UK Information Commissioner: http://information commissioner.gov.uk/eventual.aspx?id=1
- Electronic Frontier Foundation: http://www.eff.org/pub/Privacy/
- American Civil Liberties Union: http://www.aclu.org/Privacy/PrivacyMain.cfm
- Center for Democracy and Technology: http://www.cdt.org/privacy/
- Ontario Information and Privacy Commissioner: http://www.ipc.on.ca/scripts/index
- Australian Privacy Commissioner: http://www.privacy.gov.au/
- Canadian privacy Commissioner: http://www.ipcon.ca