THE DATA PROTECTION ACTS and The Work Place – Employer Obligations (Northern Ireland and the Republic of Ireland)

An examination of the Data Protection Acts by Brian Morgan Solicitor of Morgan McManus, Solicitors, The Diamond, Clones, Co. Monaghan and 12 Paget Lane, Enniskillen, Co. Fermanagh with suggestions on procedures which should be adopted by Employers to comply with the Acts.

While the relevant Data Protection Law is applied in Northern Ireland under the Data Protection Act 1998 which came into force on the 1st of March 2000 (repealing the Data Protection Act 1984) and the relevant Law in the Republic of Ireland is the Data Protection Act 1988 as amended by the Data Protection Act 2003, which came into force on the 1st of July 2003, fortunately the NI Act and the ROI Act are the product of one EC Directive namely the EU Directive 95/46/EC on the Protection of Individuals with regard to the processing of personal and the free movement of such Data.

The most important change brought about by the new Acts is the fact that they now cover manual Data. It is important to understand the following definitions which apply under the Acts:

- "Data" means information in the form of which can be processed.
- "Manual Data" means information which is kept as part of a relevant filing system or with the intention that it should form part of a relevant filing system. Effectively, "manual" means paper data.
- "Relevant filing system" means any set of information that, while not computerised, is structured by reference to individuals, or by reference to criteria relating to individuals, so that specific information relating to a particular individual is readily accessible.
- "Personal Data" means Data relating to a living individual.
- "A Data Subject" is an individual who is the subject of personal Data.
- A "Data Controller" is the person who controls the content and use of personal Data.
- A "Data Processor" is a person who processes personal Data on behalf of a Data Controller (e.g., A Pension Company processing employee details on behalf of its instructing Employer Company).

Generally, Data Protection is the safeguarding of privacy rights of individuals in relation to the processing of their personal Data. The Data Protection Acts give the individual rights to this personal information and impose obligations on the Data Controllers. On payment of a nominal fee the individual is entitled to serve a "Subject Access Request" on the Data Controller seeking all

information held by the Data Controller on that individual. Failure to furnish information or the delivery of inaccurate information can result in a Complaint to the Data Commissioner. The individual is also entitled to issue Court proceedings against the Data Controller in the event that such default causes damage resulting in distress to the individual.

For the purpose of this Discussion the Data Protection Acts as enacted in both Jurisdictions will simply be referred to as “The Data Protection Acts”. Whereas the relevant Commissioner in Northern Ireland is the Information Commissioner and in the Republic of Ireland is the Data Protection Commissioner, each of these Office Holders will be referred to as “The Commissioner”.

In an employment context, the term ‘personal data’ includes not only facts and opinions about a particular employee (the ‘data subject’) but also information about the employer's (the ‘data controller's') intentions in respect of that employee.

The Data Protection Act lays down rules concerning the processing of 'sensitive personal data' - meaning data about an individual's racial or ethnic origins, political opinions, religious or other beliefs, trade union membership, health, sex life or sexual orientation, criminal proceedings or convictions.

Data subjects (for example employees) have the right to be told about and to be provided with intelligible copies of any personal data held on computer or in a paper-based filing system. They also have the right to apply to the Civil Courts for an order directing the data controller (the relevant employer) to rectify, block, erase or destroy any such data that is inaccurate.

Transitional arrangements exempt manual or paper-based records held in a ‘relevant filing system' from full compliance until 24 October 2007 (both in ROI and NI). However, the right of employees to access personal data held on their files came into force on 24 October 2001 in NI and on the 1st July 2003 in ROI.

The Commissioner has significant powers under the Data Protection Act and may serve an ‘enforcement notice' on any employer that has contravened any of the eight ‘data protection principles' embodied in the Act.

The EU Directive should have been implemented in both NI and ROI by 24 October 1998. However, the Directive *does* allow for two transitional provisions. Since 24 October 2001 in Northern Ireland and the 1st July 2003 in the Republic of Ireland it has been necessary for personal data stored and processed on computer to comply fully with the Directive's provisions. To a limited extent, it has also been necessary for data held in manual filing systems to comply since that date.

However, manual filing systems in existence before 24 October 1998 need not comply fully with the Directive until 12 years from the date on which the Directive itself was adopted. Those 12 years expire on 23 October 2007.

The Information Commissioner in the UK issued the first part of a Code of Practice on data protection in employment on 14 March 2002 (the Employment Practices Data Protection Code Part 1: Recruitment and Selection), the second part on 3 September 2002 (the Employment Practices Data Protection Code Part 2: Records Management) and, after a review to make it more user friendly, the third part on 11 June 2003 (the Employment Practices Data Protection Code Part 3: Monitoring at Work). All three are available at www.dataprotection.gov.uk . Part 4 is not expected to be published until 2004. Once Part 4 has been issued, Parts 1 and 2 will be updated to ensure that the style is consistent across all four parts. No part of the Code will be admissible in an employment tribunal until all four parts have been published. These UK Codes are very useful for consideration by ROI employers in the implementation of their Data Protection Codes.

Meaning of Terms

The Data Protection Act 1998 applies to personal data held and processed by employers, credit reference agencies, banks, financial institutions, insurance and mail order companies, trade unions, political organisations, educational and examining bodies, and so on. As this Discussion deals solely with the processing of personal data in the context of the employee/employee relationship, the terms ‘data controller' and ‘data subject' in the text that follows refer, respectively, to ‘employers' and ‘employees'. Furthermore, the term ‘employee' encompasses any worker who undertakes to do or perform personally any work or services for an employer.

Manual or paper-based files

With the coming into force of the Data Protection Act 1998 in NI and the Data Protection Act 2003 in ROI, the rules which applied under the previous Data Protection Acts in relation to computerised records apply not only to computerised records but also to data held in a ‘relevant filing system'; that is to say, in any manual or paper-based filing system that is structured either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible. This would include a Personnel File.

Meaning of ‘personal data'

In the employment context, the expression ‘personal data' means data relating to a ‘living individual' (an employee) who can be identified from that data or from that and any other information held by the employer (the 'data controller'), or that is likely to come into the employer's possession. It also includes any expression of opinion and any indication of the employer's

intentions (or that of any other person within the employing organisation) in respect of that employee - whether contained in (or attached to) a letter, memorandum, report, certificate or other document, or held in a paper-based file, on computer, or by any other automated or non-automated means.

Although the expression 'personal data' includes an indication of an employer's intentions in respect of a particular individual, this does not mean that an employee has the right to access information (computerised or otherwise) concerning a proposed pay rise, promotion or transfer, or to access information indicating that he or she has been earmarked for further training, downgrading or redundancy.

The Act clearly states that any personal data ‘processed for the purposes of management forecasting or management planning' may be withheld if disclosing it would be likely to prejudice the conduct of the employer's business. Nor do employees have the right to access personal data which contains information concerning their employer's bargaining position in relation to negotiations or discussions about employee pay and benefits or the like.

Meaning of 'sensitive personal data'

The Data Protection Act also lays down rules concerning the ‘processing' of so-called ‘sensitive personal data'; that is to say, data which consists of information about an employee's:

- racial or ethnic origins;
- political opinions;
- religious beliefs;
- trade union membership (or non-membership);
- physical or mental health or condition;
- sex life or sexual orientation;
- criminal (or alleged criminal) activities;
- criminal proceedings, criminal convictions (or any sentences imposed by the courts).

Sensitive personal data must not be held on an employee's personal file without his or her express consent - unless held in compliance with an employer's legal obligations (for example under health and safety legislation) or to protect the employee's vital interests (for example under Equality Legislation).

Such data may also be retained for so long as may be necessary, for the purpose of defending a complaint of unlawful discrimination on grounds of sex, race, disability or trade union membership (or non-membership), or (so long as appropriate safeguards are in place) for reviewing, monitoring, promoting or maintaining the employer's equal opportunities policy.
Sensitive personal data volunteered on a job application form or during an employment interview (for example concerning a 'spent' conviction) or held

with the express consent of the employee in question (for whatever reason) should be deleted from the employee's personal file, unless retained for legal reasons or in connection with any legal proceedings.

It may be necessary to retain health records if legislation precludes the employment (or continued employment) of people in specified occupations or in work involving exposure to certain hazardous substances (for example lead or ionising radiations).

If a job application form requires a job applicant to provide information which could be characterised as ‘sensitive personal data', the form should explain the employer's reasons for requiring that information, together with an assurance that the information will be held in the strictest confidence; that (in keeping with the applicant's rights under the Data Protection Act) it will not be disclosed or otherwise made available to any unauthorised third party; and that it will be destroyed if the candidate's application for employment is unsuccessful. The same rule applies to ‘sensitive personal data' volunteered by a job applicant in a CV or similar document.

Meaning of ‘processing'

In an employment context, personal data is ‘processed' if it is obtained, collated, stored, retrieved or used by an employer for any purpose. Personal data held on computerised or paper-based files is normally used to monitor an employee's conduct, performance and progress within the employing organisation. It may also include reports from managers and supervisors and information concerning an employee's occupational and academic achievements, response to in-house and external training, health, attendance and disciplinary record, etc - leading to decisions about a pay rise, promotion, transfer, further training and development, disciplinary action, dismissal, selection for redundancy, and so on.

Some of that information will comprise sensitive personal data. Data extracted from an employee's personal file for statistical purposes (for example to measure absence and attendance levels, labour turnover and the like) will not fall within the definition of ‘personal data' so long as it does not contain the names or identities of individual employees.

Duties of employers

Personal data must be accurate, adequate and relevant; must not be disclosed to unauthorised third parties without the express consent of the ‘data subject' (the employee); must be kept up to date; must be processed fairly and lawfully; and must not be held for longer than is strictly necessary. This is known as the “eight data protection principles”.

However, the Data Protection Act allows that certain personal data volunteered by a job applicant or existing employee needs to be held on file for contractual or legal reasons, consistent (in the latter case) with an

employer's duties and liabilities under legislation such as Employment and Health and Safety Legislation.

Evidence of an employee's entitlement to parental or maternity leave, time off for dependants, annual holidays, etc must also be retained for obvious reasons. An employer would be justified in keeping documentary evidence relating to an employee's dismissal (for whatever reason) against the possibility of a complaint of unfair or unlawful dismissal or an action for damages arising out the employer's alleged negligence or breach of a statutory duty.

The same would be true of allegations of sexual or racial harassment or of an employer's failure to make reasonable adjustments to accommodate a disabled employee. Attendance records (supported by doctors' sick notes, accident reports, etc) must be maintained for that same reason, as must records of disciplinary warnings and hearings.

Keeping details of an employee's age, nationality, marital status, parenthood, next of kin, home address, telephone number, bank account, etc can be justified on a variety of practical and legal grounds (for example to comply with age limits on working hours and periods of employment, in the case of accidents and emergencies, and for the purposes of the national minimum wage, payroll, pensions).

The eight data protection principles

The Data Protection Act lists eight data protection principles relating to the processing of personal data held on manual or computerised filing systems. Thus, personal data held on an employee's personal file or on any associated or computerised record:

- must be processed fairly and lawfully, either with the employee's consent, or for contractual or legal reasons, or in the employer's legitimate interests; or to protect the employee's vital interests; and, in the case of 'sensitive personal data', not without the employee's explicit consent - unless that data is held in compliance with any statutory duty, or to protect the employee's vital interests, or for the purposes of legal proceedings, or for medical purposes or (in the case of data concerning an employee's racial or ethnic origins) for the purposes of identifying, monitoring, promoting or maintaining the employer's equal opportunities policy;

- must be obtained only for one or more specified and lawful purposes, and must not be further processed in any manner incompatible with that purpose or purposes;

- must be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;

- must be accurate and, where necessary, kept up to date;

- must not be kept for longer than strictly necessary (but, again, subject to any legal requirements to the contrary);

- must be processed in accordance with the 'subject access' rights of employees under the Data Protection Act 1998;

- must be protected (by 'appropriate technical and organisational measures') against unauthorised or unlawful processing or disclosure, and against accidental loss, damage or destruction;

- must not be transferred to any country or territory outside the European Economic Area (EEA) (for example in connection with a transfer or secondment overseas) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

I do not propose, for the purpose of this Discussion, to outline what should/should not be retained on an Employee File. This will be the subject matter of another Paper (on another day!).

Subject access rights

The rights of employees (as data subjects) in relation to personal data held by their employer are explained in the Data Protection Act. Briefly, employees have the right (on payment of a fee of up to £10/€6.35) to write to their employer asking for details of any personal data held on computer or in their personnel file or elsewhere, and to be told why that data is being held. They also have the right to be provided with hard copies of all such data (which, in the case of computer-based records, must be translated into an intelligible form). If personal data processed by computer for the purpose of evaluating an employee's performance at work, conduct or reliability constitutes the sole basis for any decision significantly affecting that employee, the employee must be informed of the logic involved in that decision taking.

Finally, an employer need not comply with an employee's request for information if doing so would disclose information relating to another individual who could be identified from that information or as the source of that information - unless that other individual has consented to the disclosure or it is reasonable in all the circumstances to provide that information without the consent of that other individual.

However, this is not to be construed as excusing employers from providing such information if they can do so without disclosing the identity of that other individual, whether by the omission of a name or other identifying particulars, or otherwise.

An employer has 40 days within which to respond to an employee's request for information concerning personal data held on computer or in a manual file; but need not do so a second time if there is too short an interval between it and the employer's earlier request for the same information.

The reasonableness of an employer's refusal to provide the same information on a second or subsequent occasion will be determined by the nature and purpose of the information in question, and the frequency with which it is altered or updated. In the final analysis, it will be for a court to decide whether or not an employer has failed to comply with a request for information or whether it was reasonable for an employer to refuse to comply with a second request for identical or similar information

Refusal of Right to Access

While the specific sections of the relevant NI/UK and ROI Acts should be examined, there are certain circumstances under which the Data Controller is not obliged to grant an employee a right to access:

- If by disclosing the personal data he/she would disclose information about a third party. Access to such information is only permitted if the third party can be rendered unidentifiable by removing items such as his/her name.
- The Minister for Justice ROI/The Health Order UK (SI 2000 No. 413) may deny access to Health and Social Work Data if access could prove harmful to the Data subject.
- Where access to Data and specific cases could prejudice matters in relation to money payable to the State or investigation into offences committed.
- Where the access would interfere with the ability to maintain security and order in prisons and other places of detention.
- If the information is kept to fulfil statutory duties/protecting the public against financial loss. This mainly concerns financial institutions.
- To protect the International Relations of the State.
- Where the data contains estimates made by Data Controllers of their liability in relation to claims for compensation, where access could prejudice the rights of the Data Controllers.
- Data held purely for research or statistical purposes.
- Back-up Data held solely to replace other Data.
- Data under a “legal professional privilege”. For example, Data given by a client to his lawyer regarding a Third Party cannot be accessed by the Third Party.

If information is refused, the Data Controller must inform the employee of the reasons for the refusal and that he has the right to complain to the Commissioner.

Access to medical reports: an employer must not approach an employee's (or worker's) GP for information about his or her state of health without first obtaining the employee's consent (and in Northern Ireland reminding that employee of his or her rights under the Access to Medical Reports Act 1988).

In Northern Ireland, under the Access to Medical Reports Act, the employee has the legal right to insist on seeing a copy of the report before it is relayed to the employer and to ask the doctor in question to remove information that the employee considers to be damaging or irrelevant. This obligation can probably also be implied into ROI law insofar as a Doctor also has duties to his patient under the Data Protection Acts. That same right does not extend to reports prepared by a company doctor or a doctor nominated and paid for by the employer.

Many employers make offers of employment conditional on the receipt of a satisfactory medical report. Annual post-employment health checks are also commonplace in larger organisations. Even so, the processing of information gleaned from such reports must not be disclosed to unauthorised third parties in keeping with employees' rights under the Data Protection Act 1998.

Rights in relation to automated decision taking: employees may write to their employer at any time requiring it to ensure that computer software used to evaluate their performance, reliability or conduct at work will not constitute the sole basis for any decision significantly affecting their employment or continued employment.

Regardless of any such prior notice, an employer is duty bound to notify an employee, as soon as is reasonably practicable, of any significant decision affecting that employee that has been taken solely on that basis. The employee may respond in writing within the following 21 days asking the employer to reconsider that decision or to take a new decision otherwise than on that basis. An employer that receives a letter couched in those terms must reply within the next 21 days specifying the steps it intends to take to comply with the employee's request. What this means, in effect, is that human judgment must play a part in any significant decision-taking exercise.

However, there are exceptions to this rule. Computers may be used as the sole basis for deciding whether or not to offer employment to a particular job applicant.

References

As a rule of thumb, employees have the right to see and be provided with copies of references supplied by former employers. In responding to any such request, an employer may consider the confidential nature of the information given in the reference, the other employer's wishes in that regard, whether or not that other employer has consented to the disclosure of that information, and whether it is possible to disclose the contents of the reference without revealing the identity of the person who issued it.

However, an employee does not have the right to see or take a copy of any reference issued by his or her present employer - whether sent to a would-be employer (to which the employee has applied for a job) or issued for educational or training purposes.

Data likely to cause damage or distress

An employee may write to his or her employer requesting that certain information be deleted from his or her file on the ground that the retention or processing of such information is likely to cause the employee substantial and unwarranted damage or distress.

The employer need not comply with any such request if the employee in question had previously consented to that information being held on his or her personal file (or if the retention of that information is necessary for contractual or legal reasons, or to protect the employee's vital interests).

Otherwise, the employer must respond within 21 days confirming that the offending information has been (or is about to be) removed or giving reasons why it considers the employee's request to be unjustified. As always, it will be for a court to decide the rights and wrongs of the employer's refusal or failure to comply.

Correction, removal or destruction of inaccurate or misleading data

With the support of the Commissioner, an employee may apply to a civil court for an order requiring the removal or destruction of any personal data held on computer or in a relevant filing system if the data is inaccurate or if it contains an expression of opinion based on inaccurate data. Data is inaccurate if it is incorrect or misleading.

The court will make such an order, and may award compensation, if satisfied that the claimant has suffered damage or distress by reason of any contravention of the requirements of the Data Protection Act unless satisfied that the defendant employer had taken such reasonable care as was necessary in the circumstances to comply with the requirement in question.

Transitional provisions

Manual or paper-based filing systems: The Data Protection Acts come into force in two stages. Eligible manual data in existence immediately before 24 October 1998 did not need to comply with the eight ‘data protection principles' nor with the sections dealing with the ‘employees' right of access to personal data) until 24 October 2001 NI/1st July 2003 ROI. Nor need it comply fully with the Data Protection Act 1998 until 24 October 2007. During that second transitional period (that is to say, the period from 24 October 2001 in NI/1st July 2003 in ROI to 23 October 2007, inclusive) employers are exempt from the first data protection principle (except the requirement that personal data

must have been obtained and be processed lawfully and fairly), and from the second, third, fourth and fifth data protection principles.

Although employees now have the right of access to personal data held in manual or paper-based files, the right to apply to a court for the correction, removal or destruction of incorrect or misleading data does not arise until 24 October 2007 (unless the court is satisfied that a claimant has suffered damage or distress because of the existence or processing of such data). It follows that employers must ensure that manual files comply with the sixth, seventh and eighth principles during that second period.

Automated or computerised systems: So far as personal data held on computer files (or stored on computer disks) is concerned, data subject to processing already under way before 24 October 1998 (but not otherwise) must now comply fully with the Data Protection Act 1998/2003.

Enforcement

An employee (as data subject) may apply to the Commissioner for an assessment as to whether any personal data processing by his or her employer has been (or is being) carried out in compliance with the Data Protection Act 1998/2003. The Information Commissioner may serve an enforcement notice if satisfied that an employer (as data controller) has contravened (or is contravening) any of the eight data protection principles.

A failure to comply with the terms of any such notice is an offence for which the penalty on summary conviction is a fine of up to £5,000 or on Indictment to an unlimited fine in Northern Ireland/€3,000 Summary Conviction in ROI but on indictment €100,000.

An Officer authorised by the Commissioner may enter premises to inspect it and any Data on that premises. He may require a Data Controller, Data Processor, or an employee thereof to disclose any Data in their control and require such persons to give information regarding procedures employed for compliance with the Acts, the sources of the Data, purposes of the Data, the persons to whom Data is disclosed and to give information regarding Data Processing equipment on the premises. He may inspect and copy information.

It is an offence to obstruct the Commissioner (or his appointed officials/agents) in the execution of his powers (including his right under warrant to enter and search premises, inspect, examine, operate and test any equipment, and to seize and remove documents).

Notification

Under the Data Protection Act, a new system of notification has replaced the previous registration procedure. Under the new arrangements, employers that process personal data about their workers purely for administrative purposes (eg payroll, recruitment and selection, promotion, training, absenteeism, statutory sick pay, statutory maternity pay, disciplinary matters, health and

safety and related reasons, etc) need no longer inform the Information Commissioner in Northern Ireland of that fact. For further information visit www.dataprotection.gov.uk or contact the Office of the Information Commissioner. Likewise, in the Republic of Ireland, the 2003 Act amends the requirements regarding who must register with the Data Protection Commissioner. Consultations are presently underway in order to establish what Organisations/Data Controllers may be exempted from the requirement of registration.

Employers must become alert to the fact that the Data Protection Act will be used by the Employee as a means of getting relevant information in an employment dispute where information prejudicial to the employer with regard to that employee will be held on File. Furthermore, the Data Protection Act will be used more regularly in the future as a nuisance tactic resulting in the employer being involved in an enormous amount of time in responding to Data Access Requests from the Employee. The Employer must bear in mind that the Employee can issue Civil Proceedings against the Employer for breach of Access Requests. It must also be borne in mind that the Employee in some cases where he finds that his Employment Claim may be unsuccessful, will still pursue a Claim under the Data Protection in order to force the Employer's hand. Again, it must be borne in mind that there is no 'one year service requirement' to entitle an Employee to make a Data Access Request.

Action point checklist

Bearing in mind the prejudicial information which could be on File if a proper audit was not carried out by the employer of his employee Files, it is very important that the Employer should immediately adopt the following checklist:

- Check recruitment and selection procedures to ensure that they comply with the Data Protection Act.

- Ensure that automated systems are not used as the sole basis for shortlisting candidates for promotion, transfer or further training. Give rejected candidates an opportunity to make representations about the objectivity, fairness and consistency of such systems.

- Scrutinise job application forms, health questionnaires, etc to ensure that the questions asked of job applicants are relevant. If necessary, accompany them with a document explaining the justification for certain questions (for example 'Are you pregnant or have you recently given birth?' or 'Do you have a disability?').

- Keep application forms, CVs and other documents provided by rejected job applicants under lock and key and destroy them within four months of the date they were informed that their application was unsuccessful. If there is a chance of an offer of employment being made at a later date, inform the candidate accordingly and ask for his or her written permission to retain that information on file.

- Where not already covered, amend Contracts of Employment to include the holding of necessary sensitive Data.

- Most workers now have the right of access to their personal file. Scrutinise files and, where necessary, launder them to remove irrelevant personal data.

- Inform employees of their rights under the Data Protection Act, in particular their right of access to the information kept about them.

- Better still, provide each employee with a copy of his or her basic personal file at least once every year. Invite the employee to identify inaccuracies and suggested amendments.

- Bear in mind that while manual data obligations will only relate in Northern Ireland to files created after the 24th October 2001 and in the Republic of Ireland to Files created after the 1st July 2003, records created prior to that date will be subject to the Manual Requirements of the Data Protection Acts in both Jurisdictions after the 24th October 2007.

- Access Requests made by Data Subjects apply to Manual Files regardless of when they were created.

- Create separate Files for each employee with minimal up-to-date information complying with the 8 principles and ensure that it is kept secure.

- Review/update Files at least once a year but ensure that records are maintained to comply with other legislation e.g Safety and Health Legislation and Employment Legislation.

- Have a Policy in place to address potential queries from employees.

- Ensure that Files have no discriminatory or derogatory comments (NB, this includes e-mails which may not have been printed and filed).

- Update your Employee Handbook to include Data Processing Practises.

- Ensure to train interviewers in Employment Law, particularly in equality legislation, as Interview Notes are subject to access.

- Ensure Disciplinary Warnings are destroyed at appropriate time advised.

- Appoint and train a Data Controller (most likely your Human Resources Manager) fully conversant with the Acts and knowing circumstances in which to refuse Right to Access.

- Exercise extreme care with e-mails.
- Exercise extreme care in preparing Performance Appraisals and Probationary Reviews – including spontaneous e-mails to colleagues concerning these matters.

- Have a clear policy on use of e-mails and agree an "E-mail Etiquette".

- Retain the right to monitor e-mail. This can be done but only on notification to the employees after the implementation of an Impact Assessment

- Use of e-mail for business purposes only.

Employers must be constantly aware of the Employees Right to issue Proceedings in Civil Courts for distress if damage is caused by inaccurate information. Public Authority Employers must be aware of the provisions of the Human Rights Act (not yet effective in ROI) and in particular Article 8 of the Human Rights Convention : "everyone has the right to respect for his private and family life, his home and his correspondence".

For further information on the relevant Data Protection Acts, consult the following websites:

UK : www.dataprotection.gov.uk (while a Northern Ireland Commissioner has been appointed, the Website for Northern Ireland has not yet been launched).

ROI: www.dataprivacy.ie

Brian Morgan
11th November 2003