

Data Protection and Employment: the UK Experience

A matter of trust and confidence?

A year after the UK Information Commissioner finalised the Employment Practices Data Protection Code, setting out comprehensive guidance for employers' management of employee personal data, the industry reaction, if not desultory has been calm and generally accepting. Employers, trade unions and individual employees do not yet appear to have encountered a specific data protection issue which is worthy of being pursued to the higher courts. Is this a sign of industry harmony, a matter of it still being early days, or perhaps a reflection of the special nature of the employment relationship (which has always been a particular focus of the Information Commissioner)? This article examines the importance of data protection in the workplace, revisiting the role of the Data Protection Act 1998 and the Information Commissioner's code and supplementary guidance in this area.

Introduction

The Data Protection Act 1998 ("the Act") has now been in force for almost eight years, and it is one of the more complex pieces of legislation that has direct impact upon the employment relationship in the UK. Although the Act imposes duties and obligations on all organisations and individuals who "process" personal data, there is little question that the most important interaction which most individuals will have with an organisation which will gather and process their personal data is with their employer.

At the very outset of the potential employment relationship, individuals will be supplying intimate details about themselves to prospective employers, ranging from basic identifying data such as name, birth date and address, to the details of educational and work history, skills qualifications and even descriptions of hobbies and leisure activities. During the employment relationship itself, the employer must manage information concerning the employee's salary, bank account, records of promotion and awards, or alternatively concerning disciplinary warnings and sanctions, sickness and accident records, and even details of an employee's racial or ethnic origin, religious beliefs, sexuality and/or disability – all matters which many employers now monitor in order to ensure compliance with equality legislation. Even after the employment relationship between a particular employer and employee has ended, employers may need to deal with written or oral reference requests from the prospective new employer.

With the possible exception of the government (viewing its separate agencies as a whole) there is no other relationship which an individual is likely to have which will involve the provision of such a high level and wide range of personal data.

The Information Commissioner has long recognised the relevance and importance of data protection in the employment relationship, and the majority of the detailed guidance which the Information Commissioner has produced focuses upon associated issues. The Data Protection

Employment Practices Code (the “Code”) was issued in 4 separate parts, and was finally completed in June 2005. The 4 parts are as follows:

1. Recruitment and selection
2. Employment records
3. Monitoring at work
4. Workers’ health

Each part of the Code sets out the Information Commissioner’s good practice recommendations on the various data protection issues which are examined. The Code is supported by supplementary guidance also issued by the Information Commissioner, which sets out more detailed notes and examples intended to assist larger organisations with the implementation of the appropriate policies and procedures.

It is important to note that the Code and the associated supplementary guidance do not have any binding legal force, but merely represent the Commissioner’s interpretation of the Act and recommendations as to how best to comply with it. In general employers are assured that compliance with the Code will ensure compliance with the Act. However, failure to follow the Code will not necessarily be a breach of the Act, but there is a risk that the Information Commissioner might take that view and bring enforcement action.

Part 1: Recruitment and selection

Part 1 of the Code is intended to cover all aspects of the recruitment and selection process for employers, from the advertising of vacancies through to the deletion of information concerning unsuccessful applicants. The Code, generally, and including in this part, takes a wide view of the scope of the guidance which needs to be provided. At times it makes recommendations on matters that arguably relate to general questions of what is good practice in selection and recruitment as opposed to the narrower issue of the handling of personal data within that process.

The Code includes reference to the following matters:

Advertising

When advertising positions, individuals should be informed of the name of the organisation to which they will be providing information, and how that information will be used.

Applications

Application forms should similarly state to whom the information is being provided and how it will be used (if this is not self-evident). In general, employers should only seek personal data that is relevant to the recruitment decision, (and not information which might be required in order to administer employment).

Verification

An applicant should be given an opportunity to make representations to the employer should any of verification checks produce discrepancies.

Short-listing

The Code suggests when short-listing applicants personal data should be used in a consistent way, and if an automated short-listing system is to be utilised as the sole basis for making a decision, applicants should be informed of that and their representations taken into account before making a final decision.

Pre-employment vetting

The process of actively making enquiries of third parties about an applicant's background and circumstances is viewed by the Code as particularly intrusive, and it is suggested that it should be confined to areas of special risk.

Retention of recruitment records

Although neither the Act nor the Code specify a time limit for retaining recruitment records, the Code does state that retention periods for recruitment records should be based on a clear business need. It reminds employers that some business needs might be served by using anonymised rather than identifiable records. For successful applicants, employers should consider carefully which information contained on an applicant form needs to be transferred to the worker's employment record. The irrelevant information should be deleted.

Information obtained by a vetting exercise should be destroyed as soon as possible, or in any case, within 6 months (although a record of the vetting or verification can be retained).

Part 2: Employment records

The Code emphasises the rights of employees to privacy (referring to Article 8 of the European Convention on Human Rights, which sets out the right to respect for private and family life) and the need for employers to take special care to comply with the special conditions which must apply if they are to gather what the Act defines as "sensitive personal data", i.e. data concerning an individual's racial or ethnic origin, political or religious beliefs,

trade union membership, personal or mental health, sexual life, or police, criminal or court records.

Equal Opportunities Monitoring

Many employees gather equal opportunities data in order to monitor their compliance with equality and diversity policies and in order to assist compliance with the now wide ranging equalities legislation. Although the Act specifically allows the processing of racial and ethnic data if it is necessary for keeping under review the existence or absence of equality of opportunity, the Code recommends only using personal data where this is necessary to carry out meaningful monitoring, suggesting that, where possible, such data should be anonymised.

Marketing

Where employers distribute information about their own products and those of third parties to their employees, the Code suggests that employees should have the opportunity to “opt out” of such arrangements.

Subject Access Requests

Like all individuals, employees have a right of access to personal data that is held regarding them. This data protection right is the one which is almost certainly the most exercised by employees. Furthermore, a subject access request is often used to obtain disclosure of documents as a precursor to potential legal proceedings brought by an employee against their employer. Employers often have to deal with wide ranging and costly subject access requests, many of which involve complex issues concerning the right to confidentiality of third parties and questions as to the extent to which the mention in emails and other documents of an employee might constitute “personal data”.

The Code sets out detailed and useful guidance on balancing the rights of employees requesting access with those of others, including the employer. Employers in any event may tend to err on the side of caution and provide as much documentation as is reasonably possible. This is in recognition of the likelihood that if any proceedings are brought, the disclosure requirements for those legal proceedings are likely to involve the provision of the same documentation. The attitude of many employers, and indeed employees, is also coloured by a strong rights-based culture in the employment field which places emphasis on individual rights. Many employers would rightly regard the right of employees to confidentiality, and the corresponding right to have their personal information handled appropriately, to be a fundamental of the employment relationship.

Mergers and Acquisitions

Mergers and acquisitions often involve disclosure of personal data in two phases. First, in due diligence prior to the final business decision being made; secondly once the decision has been made, in the run up to completion of the merger or acquisition. The Code recommends ensuring that, where possible, data is anonymised, and suggests obtaining confidentiality undertakings from the other party and assurances that data will be returned or destroyed if the merger or acquisition does not proceed.

Part 3: Monitoring at Work

The monitoring of electronic communications, and in particular, their interception is an area which is closely regulated within the UK. In general, the consent of the individuals whose communications may be intercepted is required for interception to be lawful. However, in certain circumstances, employers may be permitted to intercept email communications where there is a lawful business purpose for doing so, and where all reasonable steps have been taken to inform employees of the possibility of such interception. The Act imposes a further layer of complexity upon the monitoring framework, in that the lawfulness of and the manner in which monitoring may be carried out is restricted where it involves the gathering and handling of personal data.

Although, in general, where there is a legitimate purpose for monitoring, it is likely to be permitted by the Act, the Code once again emphasises the right of employees to a degree of privacy in the workplace. The Code suggests that an “impact assessment” regime is adopted in order to decide whether or not monitoring is appropriate in any particular circumstances. The essential issue to be determined is whether or not the adverse impact of monitoring individuals (i.e. intruding upon their privacy) is justified by the benefits to the employer and others.

In general, monitoring must be carried out in the least intrusive manner possible, and appropriate policies and communication protocols must be put in place to ensure that employees understand clearly the extent to which their activities might be monitored by their employer.

Covert monitoring which involves the gathering of personal data will only be justified where one of the specific exemptions set out in the Act applies. For example, where there are grounds for suspecting criminal activity, and informing the worker of the potential monitoring would prejudice the prevention or detection of such activity. The Code places great emphasis on ensuring that any covert monitoring is:

- linked to a particular investigation;
- barred from areas where employees would generally and reasonably expect to be private (such as toilets); and

- supervised so as to ensure that any information obtained through such monitoring is used only for the particular purpose for which it was gathered.

Part 4: Information about Workers' Health

Part 4 of the Code addresses the collection and subsequent use of information about a worker's physical and mental health or condition. Such information will constitute "sensitive personal data" under the definition contained within the Act, and the conditions regulating the gathering and use of sensitive personal data are stricter than those which apply to other personal data. The three key conditions which may justify employers gathering sensitive personal data are:

- where the processing is necessary to enable the employer to meet its legal obligations;
- where the processing is necessary for the purposes of or in connection with actual or prospective legal proceedings; and
- where the worker has given consent to the processing explicitly and freely.

The Code suggests that an impact assessment procedure is adopted to determine whether or not health information should be gathered in any particular circumstance (utilising the same procedure which is suggested when assessing the appropriateness of monitoring employees at work).

The Code draws a distinction between sickness and injury records, which contain the details of the illness or injury suffered by a worker which prevents him or her from attending work, and absence and accident records, which simply disclose the fact of the employee's absence or that an accident has occurred. The Code recommends that employers keep sickness and injury records confidential and separate from absence and accident records, whilst ensuring that the holding and use of sickness and injury records satisfies a sensible personal data condition.

Medical Examination and Testing

Special recommendations are made by the Code concerning information gathered from drug and alcohol testing and the circumstances in which such testing can take place. More generally the Code recommends that medical examinations and testing are only used to enforce the organisation's rules and standards where the employer has made sure that those rules and standards are clearly set out in a policy of which workers are aware (and the special conditions regarding sensitive personal data still need to be observed). Furthermore, where medical examinations and testing are used in the recruitment process, they should only be carried out at an appropriate point i.e. where there is a genuine likelihood that the individual being tested will be appointed. The Code emphasises that information gathered through such medical examinations should be used only for the purposes for which it was initially gathered

and should be permanently deleted once it is no longer relevant for the purposes for which it was undertaken.

Genetic Testing

Currently genetic testing is rarely (if at all) used in the employment context. However, the Code recognises that this may be a contentious and difficult issue should testing be taken up in the future as a tool by employers. The Code recommends that employers should not use genetic testing in an effort to obtain information that extrapolates a worker's future general health, but should only use it to obtain information where it is clear that a worker with a particular detectable genetic condition is likely to pose a serious safety risk to others or where it is known that a specific working environment or practice might pose specific risks to workers with particular genetic variations.

Impact of Code

The employment relationship is one which is explicitly recognised in law as personal between the employer and individual employee. Within the UK employees are extended certain statutory rights protecting them from unlawful discrimination, unfair dismissal, unlawful deduction from their wages or a breach of their employment contract. Furthermore, implied into every contract of employment is a term of mutual trust and confidence which essentially requires employers and employees to maintain good faith, and a fair and reasonable approach in relation to each other. A breach of the implied term of trust and confidence will be a fundamental breach of the employment contract, justifying its termination by the other party with immediate effect. In the case of employees, it may also amount to a constructive unfair dismissal, entitling them to statutory compensation. In these circumstances employers are, in general, careful to ensure that the implied term of trust and confidence is not breached.

In many, if not most cases, matters about which an employee would complain under the Act will also be matters where the implied term of trust and confidence would apply. For example, in order to maintain trust and confidence, employers must extend employees a degree of confidentiality concerning their affairs, and treat their personal information with care. The Act and its associated guidance including the Code have augmented and added to the rights of employees in this respect. However, they have not fundamentally changed the nature of the relationship between employer and employee, nor have they altered the likely legal claims which might be brought and the remedies which an employee could seek should they be faced with a breach of their confidentiality or misuse of their personal information. Arguably, it is for these reasons that the Code has failed to stir any significant controversy or indeed required wholesale changes of approach by employers. Where employers do not comply with their data protection obligations, employees are likely to pursue matters utilising existing remedies and the employee-friendly and relatively informal forum of the Employment Tribunal, in which it is easier to achieve significant compensation than in a standalone action alleging a breach of the Act.

The Code is highly relevant and important for determining best practice and compliance with the Act. In particular, for matters such as the handling of personal data on outsourcings and in relation to the potential export of data to foreign jurisdictions (where the implied term of trust and confidence may have little direct bearing), the Code is essential. In cases where data protection issues may be relevant, the Code is also likely to inform the determination of whether an employer has maintained trust and confidence with an aggrieved employee alleging a breach of the employment contract. However, it is the other rights which employees have, arising under their contracts of employment and from the statutory duties and obligations imposed upon employers specific to the employment field which give rise to the key incentives driving compliance with the Act. Although, in the case of individuals working for organisations without employment rights (i.e. agency temp workers, casual workers and consultants or contractors performing services for clients), the rights created by the Act and delineated by the Code, will have a greater stand alone importance, the Code and the Act should generally not be regarded in isolation, but rather as an important contribution to the complex legal framework governing employment.

(first published in World Data Protection Report in June 2006)

James Warren is an employment lawyer at Field Fisher Waterhouse LLP

Field Fisher Waterhouse LLP 35 Vine Street London EC3N 2AA
Tel +44 (0)20 7861 4000 Fax +44 (0)20 7488 0084 e-mail info@ffw.com london@thealliancelaw.com
Web www.ffw.com www.thealliancelaw.com CDE 823

Regulated by the Law Society, Field Fisher Waterhouse LLP is a limited liability partnership registered in England and Wales with registered number OC318472. Its registered office is at 35 Vine Street, London, EC3N 2AA and a list of its members and their professional qualifications is open to inspection at this address. We use the word partner to refer to a member of Field Fisher Waterhouse LLP, or an employee or consultant with equivalent standing and qualifications.

The European Legal Alliance is an alliance of independent law firms.

London Barcelona Berlin Brussels Dublin Düsseldorf Edinburgh Essen Frankfurt Glasgow Hamburg Inverness Manchester Madrid Mantova Milan Munich Padova Paris Rome Turin Valencia Verona Vicenza Vitoria Affiliate offices: Budapest Prague