

Workplace Law Network

Data Protection: the impact on employers

White Paper

Louise Westby and Sally Andrews, Steeles Law LLP

**Published December
2008**

© Workplace Law Group 2008
All rights reserved

 www.workplacelaw.net

About the authors



Sally is a Fellow of the Institute of Legal Executives who specialises exclusively in employment law. Sally is experienced in dealing with all aspects of contentious and non-contentious employment advice for numerous corporate clients. Sally also has wide experience in discrimination cases which was developed through the handling of a large number of highly publicised pregnancy dismissal sex discrimination claims and equal pay claims against the Ministry of Defence. She is a member of the Employment

Lawyer Association and the Discrimination Law Association.



Louise Westby is a trainee solicitor with Steeles Law LLP. Louise is currently undertaking her third seat in employment law.

About Steeles Law LLP



Steeles Law LLP is an independent law firm ranked amongst the leading firms in the country. The firm acts for a diverse mix of corporate companies and organisations, charities and individuals both in the UK and internationally.

Over the last 30 years, Steeles Law has built up an impressive reputation for its commercial legal expertise. The firm is specifically recognised for the strength of its employment and immigration practitioners.

Steeles Law offers practical and commercially sensible advice on a wide range of employment law and HR issues and is appropriately resourced to handle the most complex and sensitive of problems that can occur in the workplace. In addition, Steeles Law's dedicated immigration and nationality team deals are able to advise employers and employees on the complete range of UK immigration and nationality issues.

Contact details:

t: 01603 598000

e: noremp@steeleslaw.co.uk

www.steeleslaw.co.uk

Data Protection: the impact on employers

Introduction

Before considering the impact the Data Protection Act 1998 (the Act) has on specific areas which an employer is likely to encounter consideration is given to its remit.

The Act was introduced in 2000 to cover storage of personal data manually processed provided it is in a “relevant filing system” in addition to information contained on a computer.

The manually obtained information will fall within a relevant filing system if it contains information on a worker, which is structured or indexed in such a manner that a search for specific information will reveal that information within the file almost as readily as it would be if stored on a computer.

A personnel file with the name of the worker on the front separated into chronological order holding information regarding a worker is unlikely to be in a relevant filing system, as you would have to search through the various parts of the file to locate the information. If the same file was divided into sections by dividers, splitting up the records into sickness records, training, appraisals etc it will be manual data in a relevant filing system and subject to the Act. The collection and use of personal data by businesses is protected by the Act.

“Personal data” is data relating to living individuals who can be identified from the data, or from other information which is in the possession of or likely to come into the possession of the employer. The Court of Appeal have considered the meaning of personal data within *Durrant v. Financial Services Authority* (2003) and confined this to information which relates to an individual and in such a way this affects his privacy in terms of his family life, business or in a professional capacity.

The personal data has to relate directly to an individual and be information that could be used to compromise his privacy; this would include names, addresses, telephone numbers, job titles and dates of birth.

The Act places those who “process” data under obligations. Processing could include an employer obtaining, recording, holding, using, disclosing or erasing data.

Data protection principles

The Act sets out at Schedule 1 eight key principles which must be adhered to with regards to personal data. These are:

- Number 1: Personal data should be processed fairly and lawfully. In order to adhere to the principle of fair and lawful processing the Act sets out conditions which apply:
 - the employer must ensure workers are aware of the purposes for which their information is used and must ensure processing of the data is necessary for;
 - the performance of any contract to which the data subject (the individual who the information is about) is a party to;
 - compliance with an employer's legal obligation or their legitimate interest;
 - protection of a worker's vital interests, such as medical emergencies;
 - administration of justice or functions of the Crown which are public in nature;
 - legitimate interests of the employer or third party to whom the information is disclosed. If none of these can be proven an employer can rely on a worker's consent to processing their data.
- Number 2: Personal data is to be obtained only for specified and lawful purposes and is not to be processed in a manner incompatible with this.
- Number 3: Personal data has to be adequate, relevant and not excessive in relation to the purposes for which it is being processed.
- Number 4: Personal data should be accurate and where necessary kept up to date.
- Number 5: Personal data is not to be kept for any longer than necessary for the purpose is it being processed for.
- Number 6: Personal data should be processed in accordance with the rights of data subjects.
- Number 7: Appropriate technical and organisational measures are to be taken against unauthorised or unlawful processing of personal data and against its accidental loss or destruction, or damage and
- Number 8: Personal data should not be transferred outside of the European Economic Area unless that country has adequate levels of protection in place for rights and freedoms of data subjects as to processing of their data.

Sensitive personal data

In addition the Act defines data relating to racial origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health, sexual

health, sexual life, criminal offences or criminal proceedings or convictions as sensitive personal data.

There are additional requirements when processing this data under Schedule 3 of the Act and an employer will need to comply with at least one of these plus one of the key principles highlighted above.

These include:

- obtaining an employee's specific consent to the processing, which should be the last resort, if none of the following apply;
- ensuring the processing is necessary for the performance of the employer's obligations under employment law, for example health and safety laws;
- ensuring the processing is required for the purpose of legal proceedings, obtaining legal advice, establishing or defending legal rights or for administration of justice or exercise of functions of a public nature;
- if the data relates to racial or ethnic origins this is being processed in terms of equal opportunity monitoring;
- administration of justice or exercise of certain functions of the Crown or public nature;
- medical purposes by a health professional or person with the a similar duty of confidentiality;
- research purposes which do not support decisions on individuals and are unlikely to cause substantial damage or distress;
- prevention or detection of any unlawful act to be carried out without their explicit consent; and
- provision of confidential counselling, advice, support or other service to be carried out without a worker's consent or because an employer could not obtain or reasonably be expected to obtain that consent.

The House of Lords have recently considered the question of sensitive personal data in *Common Services Agency v. Scottish Information Commissioner* and although the reasoning in this case related to disclosure regarding incidence of childhood leukaemia, it is felt to have a potential impact on the employment field. It could particularly apply regarding disclosure of how many individuals a business employs in particular jobs who have criminal convictions.

The impact on employers

To assist employers with the minefield of applying the Act in the business environment the Information Commissioner's office has published the Employment Practices Code (the Code).

Data Protection: the impact on employers

The Code is not legally binding although both criminal and civil enforcement measures will follow for failure to comply with the Act. The Code provides workable guidance on the implementation of the Act and seeks to balance a workers expectations that their personal data is handled correctly with an employer's consideration as to how best to carry on his business within the law.

The Code extends to the handling of workers personal information which falls within personal data in the Act. The concept of Worker is defined widely and protects not only employees, but job applicants, agency staff, casual staff, contractors, volunteers and trainees. It could also cover both former and current workers.

The Code suggests a practical approach to data protection and that this should be integrated within employment procedures. Rather than have a discreet process an employer is advised they could for example carry out an audit of a worker's personal information in the area of occupational health. Following on from this provision could be made for individuals within this area to safeguard worker's personal information regarding sickness procedures and to implement document security and retention policies.

The Code has an overall emphasis on managing data protection and seeks to establish a culture within a business that there should be respect for private life, data protection, security and confidentiality. It suggests this can be achieved by:

- having one person who has responsibility for data protection compliance;
- auditing personal information to establish available information and who has responsibility for it;
- making sure line managers and workers throughout the business are aware of their obligations and liabilities under the Act;
- providing for serious breaches of data protection rules to result in a disciplinary act; and
- consulting with both employees and trade union representatives as to data protection compliant procedures, although this does not fall within the employment consultation requirements.

The Code is divided into four elements covering:

- recruitment and selection;
- employment records;
- monitoring at work; and
- worker's health.

I will deal with each of these in turn:

1. Recruitment and Selection

This whole process results in gathering of a large volume of personal information, from that contained in an individual's CV to details recorded at interview.

The Code recognises that information is both sought and provided at various stages throughout this process and provides guidance on Job adverts and applications, Background checks, Interviews and short listing and Recruitment records.

Job advertisements and applications.

- If information is to be transferred to an organisation who will hold this, an employer should identify this organisation, for example this could be a recruitment agency. It is important to establish if not already known what they intend to use the information for. Are they intending to use this for marketing purposes?
- It may be your business does not want to be identified in the early stages of recruitment so you could instruct an agency to send out anonymous applications.
- Questions should be limited on an application form to those which you need to ask for the specific vacancy.
- It is important that a request is made for criminal convictions only if they are relevant to the role and for an employer to advise that in most cases any spent convictions do not need to be disclosed.

Background checks

- The Code deals with these checks in two ways, splitting these into verification involving checks by the employer of information supplied by an applicant, for example on a CV and in references and vetting which involves an employer carrying out their own investigations into a party's background from other sources.
- It makes suggestions that any background checking procedures are explained to applicants as soon as possible and that the applicants be given the opportunity to respond to any adverse details these reveal.
- In terms of Pre-employment vetting, this should be restricted to situations where there are particular risks such as under the Protection of Children Act, to specific information and to applicants who are offered the job.
- Details of criminal offences should be obtained from the Criminal Records Bureau (CRB) and an applicant should not be required to obtain a copy of their own criminal record.

2. Employment records

The Code suggests that different types of records are dealt with in specific ways. It provides some general good practice recommendations and indicates:

Data Protection: the impact on employers

- although consent is not needed to keep records an employer should ensure workers are informed of how their information is used and stored and their rights to access this;
- consider what methods are used to collect personal information and make sure these are both relevant and not too much in the circumstances;
- a system should be put in place to check the accuracy of personal information in records, there could be an option that individuals check the accuracy of their own information such as their address and emergency contacts;
- it is essential that security standards are applied which protect risks of information being lost or damaged and there may be specific risks such as transporting information on laptops or sending confidential information by email or fax; and
- individuals who have access to this information should be restricted to those who are directly involved and of a reliable nature.

The types of records it specifically makes reference to are sickness and absence, pensions and insurance, equal opportunity monitoring, marketing and publications, mergers, acquisitions and business re-organisation and disciplinary, grievance and dismissal. I will consider those areas which an employer is most likely to face.

Sickness and absence records

These records are divided up in the Code between those relating to sickness and those dealing with absence.

Sickness records are considered as Sensitive personal information under the Act and one of the additional criteria must be met on processing this information. This type of information would include a doctor's certificate or a self certification form providing details of a workers illness.

Absence records do not fall into Sensitive personal data as they should just record details of a worker's absence without reference to a specific medical condition and therefore fall outside sensitive personal data.

The Code suggests that:

- sickness and absence records should be kept separately. There is no requirement to use sickness records if absence records would suffice;
- sickness absence records should be disclosed if there is a legal obligation to do so or the worker has given clear consent; and
- only those who have an involvement in the matter should have access to sickness records.

Mergers, acquisitions and business re-organisation

The Transfer of Undertakings Protection of Employment Regulations 2006 (TUPE) which apply to an asset sale on the transfer of a business specifically requires information termed “employee liability information” to be disclosed to the new employer. This information should be provided at least two weeks before the transfer takes place or if this is not practical as soon as possible.

The information which TUPE requires to be provided to the employer is:

- the identity, which is usually the name and age of employees who will transfer;
- information in their statements of employment particulars, such as a written statement of pay, hours of work, holidays;
- information regarding any relevant collective agreements;
- details of disciplinary action taken against an employee in the last two years;
- details of grievances raised by employees in the last two years; and
- details of any legal action (before a court or employment tribunal) brought by an employer against an employee in the last two years and information about potential legal action.

The Act permits disclosure of this information as it is required by law. However both the transferee and transferor employers should apply data protection principles when handling this sensitive information. The information must be accurate, up to date and secure. The transferee must ensure the information is used for TUPE purposes only such as considering liabilities and working out how employees will be integrated into their business.

It may be wise to inform workers that their personal information is being passed to another business but if it is simply not practical to do this you could anonymise this information.

If the transferee employer requires additional information to that detailed above, it is possible to disclose this to them, however safeguards should be put in place ensuring that this is on an anonymous basis. You should also either seek the consent of the employees or ensure the transferee employer uses this information for TUPE purposes only and it is destroyed after use for this purpose.

Once the transfer takes place you will need to transfer to a large extent all your employee records. You will not need the employees’ consent to do this if the information is necessary for the purpose of the transfer and business needs of both of you. It may be worth considering whether all the information in the personnel records needs to be transferred and if there is some which can be securely destroyed.

A data compliance check could be carried out by the transferee employer on the employment records that have been transferred after the business acquisition.

It may be necessary for the transferor employer to keep some of the records regarding former employees in case of future claims and the Data Protection Act will allow this provided you have a justifiable need and it is only for as long as necessary. You should delete or destroy any information not required.

Disciplinary, grievance and dismissal

Employees are able to request access to these records under section 7 of the Act.

It is important that these records are accurate and contain sufficient detail. It is particularly important that full details of reasons for a dismissal are recorded.

On accessing workers personal information for use in either disciplinary or grievance investigations regard must be had to why this was obtained and this has to be in balance with the seriousness of the matter. For example if you obtained information from an employee because they bank with you, this could not be used in a disciplinary action unless employees have been made aware previously that it would be.

There should be a process for dealing with spent disciplinary warnings and an employee should be advised what spent means, are the warnings deleted or archived.

References

The Code only covers corporate references supplied by a member of staff of an employer and although a personal reference could refer to the work undertaken it falls outside the scope of the Code and is not subject to the Act.

A worker has no right to have access to a corporate reference given by their employer but the employer receiving the reference cannot rely on this and if it receives a request to provide the reference it must give consideration to the privacy of individuals such as the author of the reference.

An employer needs to also exercise care when a reference is requested and should not disclose to the new employer details of a workers criminal records obtained via a CRB check. The Police Act section 124 specifically refers to the fact it is a criminal offence for any registered body to disclose information via the CRB. It can also be inferred from paragraph 1.3.2 of the Code that this information should not be disclosed.

The employer is unlikely to have breached any duty of care to the new employer by failing to provide this information. The new employer would be able to easily establish this for themselves and would be the one who would bear liability for any harm caused by a new employee due to its failure to carry out CRB checks.

3. Monitoring at work

The Act does not define monitoring but the Code does describe activities to which data protection compliance will attach. These include, recording worker's telephone calls for training, keeping a log of websites in order to check if workers are downloading pornography, video evidence obtained to determine worker's are not absent due to sickness and CCTV to monitor health and safety compliance.

The Code does not attach to one-off recordings designed to keep an eye on monitoring performance such as accessing of archived records to deal with a customer complaint but does recognise that worker's have an expectation of privacy at work and provides recommendations on processing information gathered from monitoring whilst ensuring balance with worker's expectations.

The Code approaches this from two different angles, by providing an overall approach and breaking this down into more specific elements of monitoring.

The general approach

- An employer should put in place an electronic communications policy which should explain the monitoring put in place and how extensive this is. This should also deal with telephone communications.
- Individuals and workers should be aware that both outgoing and incoming calls are being monitored either by recorded message or by personal communication at the time. This obligation should also be divulged regarding emails if applicable.
- Workers should be informed if home telephone lines or mobiles provided for business use are being monitored for personal use if an employer pays partly or fully for these services.
- If possible do not monitor private communications particularly where emails are marked personal.
- If emails are checked whilst a worker is absent they should be made aware of this.
- Workers should be made aware of the length of time and the extent of information retained regarding emails and internet usage.
- The monitoring of communications is also regulated by the Regulation of Investigatory Powers Act 2000 (RIPA) and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (LBP Regulations) which control monitoring through the interception of telephone calls and the internet. This interception takes place when there is monitoring in the course of a transmission. To record a telephone conversation is an interception but to access open and filed emails would not be.

If there is an interception an employer has to obtain consent of both the sender and the recipient unless exempt under the LBP Regulations.

These exemptions include, establishing facts or compliance with regulatory requirements or company policy, such as quality control and training, preventing or detecting a crime, investigating or detecting unauthorised use of communications systems, securing effective operation of communications systems.

It is also possible to determine by monitoring, but not recording if communications are personal or business or to anonymous telephone counselling or support lines.

Video (CCTV) and audio monitoring

Employers are obliged to let both workers and visitors know that video or audio monitoring is being used and the reasons why. This should be in the form of notices unless covert monitoring is being carried out.

This monitoring should be focused on areas where there is high risk of misconduct or criminal activity, for example canteens, and there is low element of privacy.

Continuous monitoring is unlikely to be justifiable unless there are exceptional circumstances as there is a high degree of intrusion into privacy. In addition to this Code the Information Commissioner has issued a Code of Practice which provides recommendations for the general use of CCTV. This can be accessed at www.ico.gov.uk.

In-vehicle monitoring

It is unlikely to be justifiable to monitor private use of vehicles unless it is possible to halt monitoring during private use. Legal requirements to monitor such as tacographs will override data and privacy provisions.

Monitoring via information from third parties

Workers need to be aware of the information which can be used to carry out checks on them and why. Information should not be obtained because an employee is also a customer, for example a bank should not obtain credit reference checks on its employee.

4. Workers' health

At Part 4 of the Code consideration is given to both collection and use of details of a worker's mental and physical health. Details could be obtained by employers in sickness records, occupational health questionnaires and medical test results.

The Code stipulates collection of this information should be kept to a minimum and where possible qualified health professionals only should have access.

This information is likely to include sensitive personal data and one of the sensitive data processing conditions must be met (as outlined above) as well as other obligations under the Code.

Occupational health schemes

Employers should let worker's know what information is being obtained under this scheme, how it is to be used and who this is to be made available to.

Regard needs to be had to potential breaches of confidentiality if monitoring of communications takes place between worker's and any health professionals.

Medical examinations and drugs, alcohol and genetic testing

Medical examinations should only be used in recruitment if there is likelihood a candidate will be successful and applicants must be made aware at an early stage of the possibility of testing.

If the medical examination or testing ties in with enforcement of an employer's policies for example sickness, drugs or alcohol a worker must be made aware of this.

Only carry out examinations or testing on current workers if they are in a voluntary occupational health and safety programme. If this is not the case an employer has to justify the examinations or testing.

Any samples should not be obtained covertly and these or test results should not be used for reasons other than those they were obtained for. The accuracy and reliability of any testing should be uppermost.

With both alcohol and drug testing any criteria for testing must be justified and workers must be made aware of this and the consequences of the tests.

Drug and alcohol testing should not be carried out randomly apart from jobs which have a safety element and any testing should be based on safety at work rather than invasion into an individual's usage in their private life.

Genetic testing should be confined to either worker's who have a detectable genetic condition which causes a serious safety risk to other individuals or where working conditions or the environment cause a risk to workers who have a genetic condition.

Medical reports

On seeking a medical report an employer should ensure they comply with the Act and the Access to Medical Reports Act 1988.

Requests for information

In addition to the processing of data, employers are likely to come across the Act at a time when a request for information is made. Individuals have a right to obtain their own personal information under section 7 of the Act. Before complying with a request an employer can ask for a fee of up to £10 and copies of identification documents such as a driving licence and passport. Issues of identity are unlikely to pose a problem if the employee still works for them but checks should be made they are requesting the information rather than a work colleague. An employer is also entitled to request such details as needed to locate the information requested.

There is a requirement to comply with this request within 40 days unless this is subject to an exemption. If the information has details of third parties such as co-workers this should be withheld or removed although on doing so an employer should try and balance a worker's right to this information with a co-workers right to privacy.

A request could also come from a third party to disclose personal information regarding a worker, if there is for example a court order to disclose this has to be complied with but only to the extent which is necessary. There may be an obligation to disclose under an exemption under the Act, for example if the information is required to obtain legal advice. An employer should consider at this stage the rights of a worker before deciding if to disclose.

The Criminal Justice and Immigration Act 2008 provides for legislation to be introduced giving greater enforcement powers to the Information Commissioner (the Commissioner).

Once in force the Commissioner will be able to fine for serious breaches of the Act and the Secretary of State will be able to increase sanctions for unlawfully obtaining or disclosing personal data as currently set out within section 55 of the Act, to custodial sentences.

The Commissioner will be able to impose a financial penalty on data controllers (including employers) if they seriously contravene any one of the eight data protection principles and this contravention is likely to cause substantial damage or distress, this was deliberate or the data controller knew or ought to have known of the risk it was likely to cause substantial damage or distress and failed to take reasonable steps to prevent it.

Consent

An employer might at this point think in order to circumvent the complex requirements of the Act it may be an option simply to obtain a worker's consent to processing the information on all occasions.

This is unlikely to suffice as the Code stipulates limits as to when consent is appropriate.

Any consent must be given freely by a worker so they must be able to choose whether to or not and must not be penalised for failing to do so.

Before obtaining consent the worker must be informed what personal data is involved and how it is to be used. It would be wise to get this consent in writing and signed by the worker.

Conclusion

This has provided a brief overview of when an employer could encounter the Data Protection Act and practical guidance on how to deal with this, however for more detailed advice please do not hesitate to contact our employment team at noremp@steeleslaw.co.uk or on 01603 598000.