The British Psychological Society

Draft

Data Protection and Privacy Issues Relating to Psychological Testing in Employment-Related Settings

Psychological Testing Centre
St Andrews House
48 Princess Road East
Leicester LE1 7DR, UK

Tel 0116 252 9530
Fax 0116 247 0787

E-mail:
enquiry@psychtesting.org.uk

www.psychtesting.org.uk

Incorporated by Royal Charter
Registered Charity No 229642

Psychological Testing Centre
www.psychtesting.org.uk

This Briefing Note in intended to inform and advise occupational test users and organisations involved in testing and assessment processes, on data protection and data privacy issues in relation to psychological testing. While due care has been taken in providing the information and advice contained in this document, neither the author nor contributing organisations accept liability for any loss or damage caused, arising directly or indirectly, in connection with reliance on the contents of this document.

Contents

Contents *continued*

Introduction

Since 1998 there has been a new legislative framework relating to personal data privacy and protection. This legislation is important for all areas of personal data, not least the sort of data processed in the course of psychological testing and assessment. Such data includes not only the information about an individual's scores on a test but also the reports that might be generated from these scores, either by computer by human test interpreters.

EU Directive 95/46/EC

The legislative framework within which this policy is set is defined by the European Union Council Directive 95/46/EC. The full title of the directive is:

> Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

This Directive sets the requirements for personal data management throughout Europe and has been legally binding on all Member States since 24 October 1998.

The countries covered by the EU Directive are the countries of the European Economic Area (EEA). The EEA comprises the 15 member states of the European Union plus Norway, Iceland and Liechtenstein, but excludes the Channel Islands and the Isle of Man.

The Directive imposes legal requirements on organisations that might transfer personal data out of the EEA.

The purpose of the Directive is to protect 'the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data' (Article 1). It provides a minimum set of requirements that all Member States must legislate to meet.

The UK Data Protection Act (1998)

In the UK, the 1998 Data Protection Act (DPA) represents the national legislation that enforces the Directive. This is supported by a detailed draft Code of Practice on 'The use of personal data in recruitment, selection and development'. When it has been confirmed, it will have mandatory status for data processing relating to data subjects within the UK. For the present Advice, it has been assumed that this Guidance will be confirmed in its current form. Much of what follows as advice is drawn from that Code of Practice.

Key definitions

The terminology used in this Advice Note has the same meaning as that in the Directive and the UK DPA. All the following definitions are taken from Article 1 of the Directive.

1. *Personal data* is any information that relates to an identified or identifiable person (the data subject). An identifiable person is one who can be identified by reference to 'an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'. A distinction is drawn between sensitive and non-sensitive personal data. Sensitive data is information relating to racial or ethnic origin, political opinions, religious beliefs, membership of organisations, physical or mental health, sexual life, offences or alleged offences.
2. *Personal data filing systems* (or just 'filing systems') refer to any structured set of personal data. This may be geographically dispersed, or decentralized. It is a filing system if information about the person is accessible from it.
3. *Processing of data* relates to any operation carried out on the data, whether manual or automated: 'collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction'.
4. A distinction is drawn between data controllers, data processors and third parties.
    a. *The controller* is the person or other authority who determines the 'purposes and means of the processing of personal data'.
    b. *The processor*, on the other hand, is 'any person (other than an employee of the data controller) who processes the data on behalf of the data controller'.
    c. *Third parties* are any other person or authority authorized by the controller or processor to process the data.
    d. Where a data controller transfers personal data to a data processor located outside the EU, the former is referred to as the *data exporter* and the latter as the *data importer*.
5. *Recipients* are people to whom data is disclosed.

6. *A data subject's consent* is defined to mean 'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.'

In general, the obligations under the Directives and related national Acts apply to Data Controllers. They have to ensure that any Data Processor they employ enables them to fulfil their obligations.

In relation to psychological testing, the data controller may be the test user or the test user's employer, or the party for whom the testing is being carried out. Data processors are third parties who process data on behalf of data controllers. These would include providers of Internet based assessments, bureau services, fax-back scoring and interpretation, and so on. Test publishers and supplier who offer online assessment services for test users are Data Processors not Data Controllers. However, they have to ensure the systems they offer their users enable them, as Data Controllers, to meet their obligations under the Act.

It is important to note that data privacy considerations apply to any 'filing system', by which is meant any information relating to an individual that is structured in such a way as to make the information readily accessible.

> *Example: Short-listing job applicants on the basis of information provided on application forms involves the processing of personal data. The application forms will be a 'relevant filing system'. Short-listing requires consultation and use of the personal information in the relevant filing system. Similarly interviewing, on the basis of information provided on application forms, will involve processing. Interviewing is also likely to involve processing in that it usually consists, at least in part, of obtaining information about applicants and recording it in a structured form.*

Timetable for implementation

The EU Directive was issued on 24 October 1995. It took on the force of law in all Member states as of 24 October 1998 where no national legislation is in place. It takes precedence over National Legislation where that does not provide the same level of protection as the Directive. However, national legislation may go beyond the requirements of the Directive.

According to Article 32, it has immediate effect after 24 October 1998 for all new automated data processing, though data processing that is already under way at that time is exempt for a period of three years (to 24 October 2001). Manually filed data existing at the time of enactment is exempt until 24 October 2007.

These time lines apply equally to the UK DPA (1998).

Test users must therefore ensure that all their practices conform to the requirements of the Directive, at least within the EU and in countries where they process personal, identifiable data originating in the EU.

Key principles of data privacy

The EU Directive's Articles

As the EU directive provides the overarching legal framework within which the UK DPA is set, the following details focus on the EU requirements. As many test users now operate beyond the shores of the UK, it is also useful for them to be aware of what is generally applicable and what may be particular to the UK.

The Directive contains 72 recitals and 34 Articles. The key principles of the Directive are contained in the Articles 6 through 9. These state that personal data must be:

1. Processed fairly and lawfully;
2. Collected for specific purposes and not processed for purposes incompatible with those purposes. Further processing for statistical or scientific purposes is not incompatible so long as appropriate safeguards are in place to protect privacy;
3. Adequate, relevant and not excessive in relation to the purpose;
4. Accurate and kept up to date;
5. Kept in a form that permits identification of the data subjects for no longer than is necessary for the purposes for which the data were collected. It may be kept longer for scientific or statistical purposes subject to the safeguards noted in [2] above.

They also define the principles relating to the legitimacy of data processing (Article 7-9 of the EU directive):

6. A data subject must have given consent or the processing must be necessary for compliance with overriding issues (e.g. legal requirements, vital interests of the data subject, requirements in the public interest etc). The 'compliance with overriding issues' (i.e. where consent is not required) includes:

(i) the processing is **necessary**:-

a) for the performance of a contract to which the data subject is a party, or

b) for the taking of steps at the request of the data subject with a view to entering into a contract.

(ii) the processing is **necessary** to comply with any legal obligation to which the data controller is subject, other than an obligation imposed by contract;

(iii) the processing is **necessary** for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case because of prejudice to the rights and freedoms or legitimate interests of the data subject.

7. Processing of personally sensitive data (racial or ethnic origin, political opinions, religious beliefs, health, sex life etc) is defined separately. As for other personal data, either the data subject must have given his/her explicit consent to the processing or the processing must be 'necessary'. What is deemed 'necessary' for personally sensitive data is more complex than for non-sensitive data (The conditions are detailed in Appendix B). Employers are much more likely to need the consent of employees if they are processing sensitive personal data rather than non-sensitive personal data. In this case the consent must be 'explicit'. However, there will be circumstances in which sensitive personal data are commonly processed where one or more of the other conditions referred to above can be relied on.

For example, an employer holding personal data on the racial or ethnic origin of employees as a necessary part of an equal opportunities programme designed to ensure compliance with the law relating to racial discrimination is likely to satisfy conditions (i) and (iv) of those given in Appendix B as being 'necessary'.

UK Data Protection Act (1998) principles

The DPA represents the EU directive in terms of eight key principles.

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless either consent has been given or one of the conditions of necessity outlined in the Schedules to the Act has been met. (These schedules set out the conditions reviewed above in relation to the EU Directive Articles 6-9).
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose

or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects in this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area, 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.

Considerations applying to the first principle

What is fair?

The DPA makes clear that, with some limited exceptions, processing will not be fair unless the data subject has, is provided with, or has made readily available to him/her information that includes:

- the identity of the data controller;
- the purpose(s) for which his/her data are to be processed;
- other information necessary to enable the processing to be fair such as a description of any persons to whom the data will be disclosed.

The obligation to provide this information to the data subject applies whether personal data are obtained directly from the data subject or indirectly from another source.

While the 1998 DPA is too new to provide relevant case law, when considering related issues in connection with the 1984 Data Protection Act, the Data Protection Tribunal has taken the view that in deciding whether processing is fair, the most important single consideration is the interests of the data subject.

What is lawful?

There is a catch all provision that if data processing breaches another legal duty or responsibility or necessarily leads to such a breach then it will also breach the First Data Protection Principle. Legal duties and responsibilities particularly relevant to the collection and use of personal data in employer/employee relationships are:-

- The common law duty of confidence – much of the personal information held by an employer about individual employees is likely to be subject to a duty of confidence. This restricts the employer's ability to disclose the information or use it without consent, for purposes other than those for which it was provided.
- The Human Rights Act 1998 – the Act gives effect to rights and freedoms guaranteed under the European Convention on Human Rights. Public authorities including the courts and tribunals such as the Data Protection Tribunal must not act in a way that is incompatible with a Convention right unless the need to apply primary legislation leaves them with no choice. The Convention right most relevant in this context is the right to respect for private and family life (Article 8): Everyone has the right to respect for his private and family life, his home and his correspondence.

Individual rights

The Data Protection Act 1998 provides the following rights for individuals:-

1. Right of subject access;
2. Right to prevent processing likely to cause unwarranted and substantial damage or distress;
3. Right to prevent processing for the purposes of direct marketing;
4. Rights in relation to automated decision taking;
5. Right to compensation;
6. Right to rectification, blocking, erasure or destruction;
7. Right to request an assessment.

These rights are explored in more detail later in this document.

Legal remedies

Employers can be subject to legal action by employees or other individuals as well as action by the Information Commissioner for breaches of the Act. Under Section 13, individuals who suffer damage and distress as a result of any contravention of the requirements of the Act are entitled to go to court to seek compensation where the data controller is unable to prove that they had taken such care as was reasonable in all the circumstances to comply with the relevant requirement.

Individuals can also go to court for an order requiring an employer to rectify, block, erase or destroy inaccurate personal data about them or personal data that contains an expression of opinion based on inaccurate data. Furthermore, they can go to court for an

order requiring rectification, blocking etc. if they have suffered damage, entitling them to compensation under Section 13 of the Act, by reason of any contravention by an employer of any of the requirements of the Act and where there is a substantial risk of further contravention.

These risks are in addition to an individual's right to request the Information Commissioner to make an assessment as to whether processing is likely or unlikely to comply with the Act.

Advice on good practice

The advice is presented in two sections. One addresses the obligations of data controllers and the other those of data processors. The obligations on Data Controllers and Data Processors under the EU Directive and the DPA are clearly set out for the UK in the [draft] Code of Practice on 'The use of personal data in recruitment, selection and development' (Information Commissioner, 2000). The following text draws heavily from that document to ensure that the advice presented closely conforms to its provisions.

Data controller obligations

As defined earlier, the Data Controller is the person or organisation that exercises control over the personal data and determines the ways in which it will be used and processed. The data controller may be an individual, a company, or some other form of organisation. The data controller need not have physical ownership of the data, but they are responsible for issuing the instructions on how it shall be processed.

It is worth emphasising that it is data controllers who are responsible for complying with the DPA and EU Directive. It is their responsibility to notify the Information Commissioner of the processing that they are having carried out. It is to them that data subjects have recourse for any issues arising about their data or the way it is being handled. Data Controllers are liable for what is done to the personal data they control even when the actual processing is carried out for them by a data processor.

In most cases, for employment-related issues, the data controller will be the employing organisation. It is generally not an individual person. For example, the Data Protection Officer in an organisation does not determine how personal data will be processed for selection, or for promotion. Such determinations arte regarded as being functions of the organisation.

Joint data controllers and data controllers in common

It is also important to recognise that there may be cases where more than one data controller controls the processing of a set of personal data. For example, two companies within the same group sharing data on employees for the same purpose, would be jointly liable for any breach under the DPA. Data controllers who share data for different purposes are referred to as 'data controllers in common'. In this case, each is individually responsible for the processing they have carried out on the data.

Compliance with the seventh data protection principle

The Seventh Principle concerns the need for data controllers to take both organisational and technical measures to prevent unlawful processing and against accidental damage or loss of personal data. The emphasis on organisational as well as technical measures is important. It is not enough simply to rely on technical IT solutions to security issues, or to put extra locks onto personnel filing cabinets.

Organisational measures should include:

- Putting data protection and security policies in places and supporting their implementation;
- Monitoring compliance with policies and procedures;
- Ensuring all staff are aware of their rights and responsibilities under the DPA;
- Ensuring that access to data is provided only to relevant staff;
- Having appropriate disaster recovery plans in place.

Technical measures could include:

- The physical security surrounding areas where personal data is held;
- The use of lockable filing cabinets for personal data;
- The use of encryption, firewalls and password protection for computer filing systems;
- Ensuring data is protection (e.g. by encryption) when in transit;
- Guarding against loss by regular daily backups.

In many cases, the physical management of the data will be in hands of a data processor outside the data controller's organisation. It is then the responsibility of the data controller to ensure that the data processor is contractually bound to meet these requirements (see later).

In the UK, the Information Commissioner has agreed that adopting BS 7799 is a good starting point for establishing compliance with the Seventh Principle.

Standards relating to testing and assessment

The following section addresses those matters in the draft Code of Practice most likely to impact on testing and assessment. In the Code these are presented as 'standards' for data controllers to follow. Those standards in italics are advisory; those in plain typeface are ones that are intended to be mandatory. Relevant DPA Principles are indicated.

Recruitment

Employers should not collect more information than they properly need to support their processing. In particular they should not:

- Collect and hold information simply on the basis that it might come in useful one day with no clear idea how and when;
- Collect and hold information on all employees or potential employees when it is only needed on some. For example all applicants should not be asked to provide items of personal information that, in fact, will only be needed for the successful candidate.

Job advertising

- Inform individuals responding to job advertisements who they are providing their information to and how this will be used if it is not obvious *(Principle 1)*.
- Where responses are simply to obtain details of how to apply, explain any uses that go beyond despatching and keeping a short-term record of the despatch of these details *(Principle 1)*.
- Provide any explanation that is needed in the advertisement or at the start of the telephone call if telephone responses are sought *(Principle 1)*.
- If the employer is not identified in the advertisement ensure the recruitment agency is identified and that no personal data are passed from the agency to the employer *(Principle 1)*.

Job applications

- State on any application form whom the applicant is providing information for and how it will be used unless this is obvious *(Principle 1)*.
- Do not seek personal information that is not necessary to enable a recruitment decision or is overly intrusive given the nature of the job to be filled *(Principles 1 &3)*.
- If questions on criminal convictions can be justified, make clear that spent convictions do not have to be declared (unless the job being filled is covered by an exception) *(Principles 1 & 3)*.
- Inform the applicant if information about him/her is to be obtained from other

sources *(Principle 1)*.

- Explain checks that may be undertaken to verify the information provided in the application in accordance with the standards set out in the following section (2.3 Verification) *(Principle 1)*.
- If sensitive data[1] are collected, explain how these will be used and obtain a clear indication of the applicant's agreement *(Principle 1)*.
- Provide a secure method of transmission if applications are accepted on-line *(Principle 7)*.

Verification Of applicant information

- Explain to applicants the nature and extent of the checks that will be undertaken to verify the information provided. Obtain their agreement both to the release of necessary details to third parties and the provision of personal information to the employer by these third parties *(Principle 1)*.
- Do not obtain personal information from applicants and then seek to verify it solely to test their honesty unless:-
  - the requirement for honesty is a particular feature of the job to be filled, for example, because the post-holder is likely to be called on to give evidence in court, or;
  - there are clear grounds which call into question the honesty of the particular applicant from whom the information is obtained and, in both cases;
  - the information obtained is not particularly intrusive and;
  - the applicant has been informed that information supplied will be verified *(Principle 1)*.
- Where information obtained from an applicant differs from that provided by a third party give the applicant an opportunity to provide an explanation before reaching a conclusion *(Principles 1 & 4)*.
- *Do not require job applicants to exercise their right of access to information held about them by third parties as part of the recruitment process.*(This will become a legal requirement in relation to police, prison and social security contribution records when Sections 112, 113 and 115 of the Police Act come into force) *(See Section 56 of the DPA)*.

Short listing

The Data Protection Act (1998) has a particular impact on the short-listing process if it involves an element of automated decision-making. If a decision is based solely on the evaluation of attributes of an applicant by automated means there is a specific

[1] For a definition of sensitive personal data, see Appendix B.

requirement that applicants' interests must be safeguarded. This will be the case if an applicant is rejected or treated in a way that is significantly different from other applicants solely as a result of an automated process. It will not be the case if the automated process merely provides information, for example a score resulting from a psychometric test that is just one of a range of factors taken into account in a human decision. However, any automated system must process information about individuals fairly (for further details on automated decision-making, see Appendix A).

- Ensure that short-listing is carried out in a way that produces results that are objective, consistent and fair to applicants. This implies the drawing up and use of criteria for assessing applications *(Principle 1)*.
- Only use an automated system in short listing if the system can be demonstrated to produce results that are objective, consistent and fair to applicants *(Principle 1)*.
- Where an automated system using some form of evaluation is used as the sole basis for a decision to reject an applicant, inform the applicant that an automated system is used, give the applicant an opportunity to make representations, and consider these representations before a final decision is reached *(Principle 6)*.

Selection testing

The considerations are similar to those applying to short listing. It is not only automated testing that involves the processing of personal data. In so far as testing involves such processing, the testing must operate lawfully in a way that is fair to individuals. Processing includes use. Test results must therefore be used in a way that is fair to applicants. These factors imply that testing should only be carried out and results interpreted by those who are qualified to do so. If the results of automated testing are translated directly into decisions that have a significant effect, there must be safeguards. These considerations apply equally to tests of knowledge, skills, mental capacity and aptitude as to psychological testing. They also apply to medical testing that forms part of the selection process (see section 7).

- Only use methods of selection testing that can be demonstrated to produce results that are objective, consistent and fair to those being tested *(Principle 1)*.
- Ensure that psychological and other complex tests are only used and interpreted by those who have received appropriate training *(Principle 1)*.
- Where the result of an automated test is used as the sole basis for a decision to reject an applicant or to take another significant decision in the recruitment process, inform the applicant that an automated system is used, give the applicant an opportunity to make representations and consider these representations before a final decision is reached *(Principle 6)*.

Interviews

Interviews involve the processing of personal data in that personal information is collected and recorded. It is beyond the scope of the Code to set detailed standards for the proper conduct of interviews. Information collected in the interview should be relevant and not excessive for the purpose of making a recruitment decision.

- Conduct interviews in accordance with accepted good practice to ensure personal information is obtained and used fairly and lawfully *(Principle 1)*.
- Limit the recording of responses to questions to those that are relevant to and not excessive for making a recruitment decision *(Principle 3)*.
- If information is volunteered, only record and retain that which is relevant to the recruitment decision or necessary to be able to demonstrate that the decision was properly taken *(Principle 3)*.

Retention Of recruitment records

Other than for the successful applicant, recruitment records should not be retained any longer than is necessary for making an appointment and responding to any challenges to that appointment. If records are to be retained because applicants might be considered for other vacancies that arise in the future, applicants should be advised of this and given an opportunity to say no. Unless there is a reason to believe an applicant wishes to be considered again, the assumption should be that he/she has applied only for the vacancy advertised. Where records of unsuccessful applicants are maintained for management analysis, for example, to check for possible sex discrimination, they should not be kept as personal data. Information that enables an individual to be identified should be deleted from the record.

- Establish and stick to retention periods for recruitment records that are based on a clearly established business need for retention *(Principle 5)*.
- *Do not keep records for longer than*
  - applicants that are not short listed; 4 months from the date on which applicants are informed of this;
  - applicants that are short listed; 4 months from the date on which applicants are informed of the appointment decision.
- Where information is obtained in the course of verifying the details supplied by an applicant or in the course of pre-employment vetting, do not use the information for any other purpose. Keep it securely (see section 3.4) until the verification/vetting is complete. Then destroy the information, merely keeping a record that verification/vetting has been carried out and the result *(Principles 2, 5 & 7)*.

- If records are retained for future consideration in the event of a further vacancy, advise applicants and give them an opportunity to object *(Principle 1)*.

Employment records

Employers clearly need to hold records that enable them to keep under review the ability of employees to undertake the work they are employed for. They also need to hold records they might reasonably require to defend themselves, for example, in an employment tribunal. However, the risks to employees if decisions are taken or opinions formed on the basis of inaccurate or inadequate records are obvious as are the risks if records are not kept securely. Employees who have to provide personal information in connection with their employment should have the reassurance that the information will not be used for other purposes without their agreement unless there is an overriding justification. Sensitive personal data, for example information as to an employee's health or trade union membership are likely to form part of the employment record.

- Apply proper security standards, such as those identified in BS7799, that take account of the risks of unauthorised access to or accidental loss or destruction of or damage to employment records *(Principle 7)*.
- Institute a system of access controls and passwords that ensure staff access to employment records is strictly on a 'need to know' basis *(Principle 7)*.
- Keep a log of non-routine access to employment records and, as far as possible, use systems that record an audit trail of all access to computerised records whether routine or not *(Principle 7)*.
- Take steps to ensure the reliability of staff that have access to employee records *(Principle 7)*.
- Treat accessing, disclosing or otherwise using employee records without authority as a serious disciplinary offence. Make staff aware of this and also that such conduct may constitute a criminal offence *(Principle 7/Section 55)*.
- Pay particular attention to the risks of transmitting confidential employee information by e-mail or fax.

Equal Opportunities

Monitoring of ethnic origin, sex or disability is clearly an accepted employment practice provided it is used to promote equality of opportunity. The Data Protection Act does not prevent this but, in order to reduce the risk of misuse, the use of personal information about identifiable employees or applicants should be kept to a minimum.

- Do not collect information about ethnic origin, sex, disability or other personal

characteristics unless it is a legal obligation, a necessary element of an established programme for the promotion of equality of opportunity or it is otherwise needed because of some special feature of a particular job *(Principle 3)*.

- Design questions to ensure accurate data collection. For example do not limit the range of choices of ethnic origin to the extent that individuals are forced to make a choice they consider does not properly describe them *(Principle 4)*.
- Wherever possible keep information used for equal opportunities monitoring in an anonymised form so that it cannot be linked to particular employees *(Principles 1 & 3)*.

Performance review and appraisal data

Any system of staff review or appraisal is likely to involve the collection and recording of personal information. It is beyond the scope of this Code to set detailed standards for the proper conduct of review or appraisal systems. Information recorded should be relevant in that it supports or will inform employment decisions and should not be misleading.

- Operate review/appraisal systems in accordance with accepted good practice to ensure personal information is obtained and used fairly and lawfully (Principle 1).
- Limit the recording of information to that needed to support recent or future employment decisions *(Principle 3)*.
- Ensure that the record identifies the source of any comments, that opinions are not presented as facts, that information recorded is correct and not misleading and that if the employee has challenged the accuracy this is recorded *(Principles 3 & 4)*.
- *Show employees all information recorded in the review/appraisal system about them. Provide a facility whereby they can record their own observations as part of the record. Ensure these observations are taken into account whenever the record is consulted.*

In relation to access to data, care needs to be exercised over an individual gaining access to personal information belonging to third parties - as would be the case if the full data from a 360-degree feedback assessment were disclosed to one of the parties involved in it (for further details, see Access and Disclosure).

International management

There are risks to employees if personal data about them are passed to countries that either have no data protection law or have laws that offer significantly less protection than is provided in the European Union. An employer transferring employee data outside the European Economic Area must establish a basis on which to do so. Where one-off transfers are made, the consent of the employee to the transfer is the obvious basis.

Where routine transfers take place, as may be the case with multi-national groups, an alternative basis may be preferable.

- Do not transfer employee data to countries outside the EEA unless:-
  - the destination country has been designated as providing adequate protection by the European Commission[2], or;
  - the destination country is the USA and the recipient has signed up to the 'safe harbour' principles, or;
  - the employee has been told about the intended transfer and has agreed to it, or;
  - the transfer is to an organisation that acts only as a processor, the processor is reliable, the country in which it is located is stable and the required controller-processor contract is in place (see Section 3.5), or;
  - steps have been taken to ensure that taking account of all the circumstances of the transfer and the Information Commissioner's guidance on international transfers, adequate protection is provided in other ways *(Principle 8)*.
- Ensure employees are made aware of any transfers of their personal data outside the EEA *(Principle 1)*.

Access and disclosure

Issues of access and disclosure are central to the Data Protection Act. Employees, like any other individuals, have a right to know what information is kept about them. Equally they are entitled to expect that the confidentiality of this information is respected and that it is only disclosed in limited circumstances.

Subject access

A subject access request is any written (including e-mail) request from a prospective, current, past employee or any other person that indicates the person wants to know what information is kept about him/her. Employers can charge up to £10 for responding to each request and can ask for information that helps them locate the records, for example dates of employment.

Employees are free to agree alternative arrangements with employers. For example, an employee might agree to withdraw a formal request if the employer provides particular information the employee is concerned about free of charge. There are some exemptions

[2] A list of designated countries is published on the Data Protection Commissioner's Website www.dataprotection.gov.uk

from the subject access right, one of which is particularly relevant to employment. Information kept for management planning or forecasting can be withheld where supplying it would prejudice the employer's business.

- Have in place a system that enables you to locate all the information about an employee and provide him/her with a copy of that information promptly and in any event within 40 days of receiving a subject access request *(Principle 6)*.
- Check the identity of anyone making a subject access request to ensure information is only given to the person entitled to it *(Principle 6)*.
- In responding to a subject access request:-
  - tell the employee whether you keep any personal information about him/her;
  - if you do, give the employee a description of the type of information you keep, the purposes you use it for and the types of organisations you pass it on to;
  - show the employee all the information you keep about him/her, explaining any code or other unintelligible terms used;
  - provide this information in a hard copy or readily readable, permanent electronic form unless doing so involves you in an effort that outweighs any possible benefit to the employee or the employee agrees to receive it in some other way;
  - provide the employee with any additional information you have indicating the source of the information you keep about him/her *(Principle 6)*.
- Take care where the information you keep about an employee or details of its source includes information about another person such as a manager or a supervisor who has not agreed to its disclosure. If the information identifies the other person directly or will enable the employee to identify them decide whether it is reasonable to release it *(Principle 6)*.
- In deciding whether to release such third party information follow the process set out below. *(Principle 6)*.
- Always release as much information as is possible, without enabling the third party to be identified even if that information actually relates to the third party as well as the employee *(Principle 6)*.

Conflicts with the privacy of third parties

A particular problem arises for employers who may find that in complying with a subject access request they will disclose information relating to an individual other than the employee making the request, who can be identified from the information. This includes situations where the information is such that it enables the other individual to be identified as its source. This problem is likely to arise in relation to references received by

an employer and where information identifying others such as colleagues or managers appears in an employee's record (e.g. for 360 degree feedback).

The Act recognises the problem and sets out only two circumstances in which the employer is obliged to comply with the subject access request in such circumstances, namely:

- where the other individual has consented to the disclosure of the information, or;
- where it is reasonable in all the circumstances to comply with the request without the consent of the other individual.

The Act assists in interpreting whether it is reasonable in all the circumstances to comply with the request without the consent of the other individual concerned. In deciding this question regard shall be had, in particular, to:

- any duty of confidentiality owed to the other individual;
- any steps taken by the employer with a view to seeking the consent of the other individual;
- whether the other individual is capable of giving consent, and;
- any express refusal of consent by the other individual.

If an employer is satisfied that the employee making the request will not be able to identify the other individual from the information, taking into account any other information which, in the reasonable belief of the employer, is likely to be in (or to come into) the possession of the employee, then the employer must provide the information.

References

There is a special exemption from the right of access to a confidential reference in the hands of the person who gave it. However, good data protection practice is to be as open as possible with employees about information that relates to them. They should be able to challenge information that they consider to be wrong or misleading particularly when, as in the case of a reference, inaccurate information may have an adverse impact on them. When a confidential reference is in the hands of the recipient there is no blanket exemption from the right of access although the recipient is entitled to take steps to protect the identity of third parties such as the author of the reference.

- *Allow access by employees to confidential references written about them. Only withhold information that if given to the employee would be likely to:-*
  - *result in harm to the author of the reference or some other person;*
  - *reveal information provided by a person other than a supervisor or manager of the*

employee who would not have expected it to be revealed.

- Allow access to references received in so far as the identity of a third party, such as the author of the reference, is not revealed *(Principle 6)*.
- In deciding whether to release third party information, follow the process set out in Appendix 1. Bear in mind that the release of information that identifies the author of a reference in his/her business capacity rather than in a private capacity is less likely to intrude on his/her private life *(Principle 6)*.
- Do not provide confidential references on employees unless you are sure they have given their consent to your disclosure either directly to you or to a third party you can trust *(Principles 1 & 7)*.

Retention of personal data records

- Establish and stick to standard retention times for the various categories of information likely to be held on the records of employees and former employees *(Principle 5)*.
- Base standard retention times on a clearly established business need for retention:-
  - bear in mind that information should not be retained simply on the basis it might come in useful one day;
  - establish how often particular categories of information are actually accessed after say 2,3,4 and 5 years;
  - consider what realistically would be the consequences for your business, for employees and former employees and for others if information that is accessed only very occasionally were no longer to be available;
  - treat items of information individually or in logical groupings. Do not retain all the information in a record simply because there is a need to retain some of it *(Principle 5)*.
- Have in place a system, whether automated or manual, to ensure that records are not kept beyond the standard retention time unless there is a justified business reason for doing so *(Principle 5)*.
- If records are maintained for management analysis, for example, to check for possible unlawful discrimination, delete the information which enables individuals to be identified *(Principle 5)*.
- Ensure records that are no longer required are properly and securely disposed of. Take particular care to ensure that when computer records are deleted the system does not retain a copy and that there are secure arrangements for the disposal of paper records *(Principle 7)*.

- *Treat the following as guidelines for retention times in the absence of a specific business case supporting a longer period.*

- *Application form*	*Duration of employment*
- *References received*	*1 year*
- *Annual appraisal/assessment records*	*5 years*

Data processors

At noted above, Data Processors are organisations or individuals, other than employees, that do not themselves decide why employee data are processed. They merely provide an employer with a processing service that operates under the employer's instructions. Examples could include:

- An application service provider (data processor) who hosts an internet-based assessment system that an organisation (data controller) uses for a 360-degree feedback project for its staff,
- A service provider (data processor) that manages a fax-back bureau service for scoring paper-and-pencil tests for career guidance consultants (data controllers).

In all cases, it is the data controller's responsibility to ensure that:

- Any data processor they choose adopts appropriate security measures both in terms of the technology it uses and how it is managed *(Principle 7)*.
- The processor actually complies with these measures *(Principle 7)*.
- They have in place a written contract with any processor that requires it to:
  - process personal information only on the data controller's instructions;
  - maintain appropriate security *(Principle 7)*.

Obligations On Processors Of Test Data

The DPA requires that agreement between a data controller and data processor is evidenced in writing. Where the amount of data being handles is small and the relationship short-term, a letter of agreement or terms of business document may be sufficient. Such letters or terms need to cover the issues of ensuring security and only processing data under the instructions of the data controller.

For more substantial data processing relationships, there will normally need to be a formal contract containing clauses dealing specifically with

data protection issues. It is in the interest of both parties to ensure that data processing is governed by a contract binding the data processor to the relevant data controller and stipulating in particular:

1. The data controller's requirements with respect to:
    a. The conditions under which data may be released to data subjects, recipients, or third parties.
    b. the period of time for which data should be retained in identifiable form,
    c. whether statistical or scientific use may be made by the data processor of the data once that time has passed and it has been render un-identifiable.
2. The guarantees provided by the data processor to ensure that the data controller can meet his/her obligation to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
    a. That the measures adopted to provide these guarantees shall, having regard to the state of the art and the cost of their implementation, ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.
    b. That the obligations in respect of technical security measures and organizational measures governing the processing to be carried out that are incumbent on the data controller shall also be incumbent on the data processor.
3. That the data processor shall not process personal data except on instructions from the data controller. To ensure that this requirement is met, the contract must include signed confirmation by the data controller that instructions have been provided to carry out the processing that the data processor deems necessary in order to produce the outputs requested by the data controller.
4. That the specific obligations the data processor must meet shall be those defined by legislation in the country within which the data processing is carried out.
5. That where the country in which the data is processed lies outside the European Economic Areas (EEA), the data processor will ensure that the conditions are such that the requirements of the EU Directive are met in full and that the data controller is able to meet all their obligations under the EU Directive and local national law.

Data Processing System Requirements

It is the responsibility of the data controller to ensure that data subjects know who the data controller is. The data processor must ensure that the data controller can meet this

responsibility by providing the necessary information through email or other form of notification for all assessment situations where the data subject may be initially unknown to the data controller or may not be a member of the data controller's organisation.

Data processors must ensure that their data processing systems enable data subjects who are asked to enter personal data into such a system to be advised by the data controller about:

- The identify of their data controller;
- The purposes for which the data are intended;
- The recipients or categories of recipients of the data;
- The existence of the right of access to the data and the right to rectify it;
- Whether responses are voluntary or obligatory;
- The consequences for the data subject of failure to respond.

Data processors must ensure that their data processing systems enable the data controller to fulfil his/her responsibility to provide data subjects with a report containing the following information:

- A list of the data subject's personal data held on the system, together with information about its status, dates of access and the identities of recipients;
- Confirmation as to whether data are being processed and the purposes of the processing;
- Communication in an intelligible form of the data that is undergoing processing;
- A description of the logic involved in any automatic processing of their data.

Data processing systems should only enable automated individual decisions to be made where that decision is made in the course of the data subject entering into or performing a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his/her legitimate interests.

Data processors should provide data controllers with the capability of overriding automated decision-making functions and of providing individual data subjects with an explanation of the logic underlying the decision-making process, should they request this. Subject to the data controller receiving a legitimate request from a data subject, the data processor must be able to ensure that it can rectify, erase or block access to data relating to that data subject, where the processing does not comply with the Directive, and

provide confirmation of the same to the data controller (who, in turn, may be obliged to notify third parties).

General Advice for Data Processors

In the field of testing and assessment, there are various individuals and organisations offering data processing services. These range from individual psychologists and other consultants who provide testing and assessment services, to publishers who manage bureau scoring or internet-based assessment.

Organisations that provide data processing services to various organisations need to have procedures in place to ensure they can assure their client data controllers that they can meet their obligations under the DPA.

Organisational and general business issues:

All organisations working in the personal data processing field should:

- Appoint an individual to take control of data protection responsibilities;
- Provide a contact point for data protection enquires from client data controllers;
- Have a data protection policy and compliance procedures in place, including data retention and data destruction;
- Ensure that staff are trained in data protection issues and compliance procedures;
- Take steps to ensure the reliability of staff who have access to personal data and make a breach of data protection an explicit disciplinary offence;
- Have procedures in place to restrict the access of staff who do not have authority.
- Prepare a standard statement describing the levels of compliance they can provide for data controllers;
- Maintain evidence and records of compliance;
- Offer data controllers access for audit purposes;
- Have a standard set of clauses for use in contracts with data controllers;
- Ensure that contracts with subcontractors pass on any relevant liabilities;
- Apply the same requirements for compliance to subcontractors as data controllers apply;

Technical security issues

All organisations working in the personal data processing field should:

- Ensure technical security levels are sufficient and appropriate to the sensitivity of the personal data held;
- Have technical measures in place to restrict access to personal data;

- Have technical measures in place to ensure security of data during transit;
- Ensure compliance of subcontractors with all security requirements;

Physical security

All organisations working in the personal data processing field should:

- Ensure that the premises on which the data are held are secure and access to non-authorised people is restricted;
- Ensure that adequate monitoring (e.g. CCTV, 24 hour security) procedures are I place;
- Ensure that non-automated data storage is held securely (e.g. in locked cabinets);
- Ensure that copies of data, print-outs, personal reports, obsolete back-up tapes etc are disposed of securely.

For detailed guidance on the contractual relationships between data processors and data controllers see McKilligan (2001).

Transfer of data out of the European Economic Area

The countries covered by the EU directive are the countries of the European Economic Area (the EEA comprises the 15 member states of the European Union plus Norway, Iceland and Liechtenstein, but excludes the Channel Islands and the Isle of Man).

Whenever data is transferred to a country outside the EEA special contractual arrangements need to be put in place. The EU Directive (DPA's Eighth Principle) restricts the transfer of personal data out of the EEA to those countries where an adequate level of protection can be established for the data. Thus, A data controller should only transfer data for processing out of the EEA to a country where the level of protection provided, considered in relation to the nature of the data, the purposes of the processing, and the security measures in place, is sufficient to meet the requirements of the EU Directive.

The contractual arrangements needed where a data processor manages a data controllers data outside the EEA must provide for additional levels of protection for the data. In particular, they need to contain a provision for data subjects to be able to enforce the contract directly with the data processor (for transfers within the EEA, the data subjects can only enforce provisions with the data controller).

These additional requirements may not be necessary if:

1. The transfer is made to an EC approved country (currently the list includes Switzerland and Hungary, and Canada is being considered for inclusion).
2. The data controller has signed up to 'safe harbour' principles (currently, registration as a 'safe harbour' is only an option in the USA). Safe harbour arrangements have been agreed by the EU Commission to meet the requirements of Article 25 of the EU Directive

Personal data should only be transferred to a country outside the EEA that does not ensure an adequate level of protection on condition that:

- The data subject has given his/her consent unambiguously to the proposed transfer; or
- The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request.

The EU (1 July, 2001) has produced a draft set of clauses for contracts between data processors and data controllers where the former is acting as a data importer and the latter as a data exported, with respect to the EU. This draft makes clear that the law that shall apply to the contract between controller and processor shall be the law of the country in which the data controller is located (for further details, see References).
A revised draft set of model clauses, based on Articles 25 and 26 of the Directive, has also been produced by the Confederation of British Industry (CBI, 2001).

References and sources of further information

EU directive 95/46/EC

The full text of the EC Directive 95/46/EC can be found on:
http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html

EU Commission Decision (draft, July 2001). Standard Contractual Clauses under article 26(4) of Directive 95/46/EC for the transfer of personal data to processors established in third countries. Copies of the draft can be fund at:
http://europa.eu.int/comm/internal_market/en/dataprot/news/sccprocessors.htm

UK Data Protection Act

The UK Data Protection Act (1998) can be found on:
http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The (draft) Code of Practice for the UK DPA relating to Employment can be found on: **http://wood.ccta.gov.uk/dpr/dpdoc.nsf**

The address of the Information Commissioner's Office (formerly known as the Data Protection Commissioner) is:
Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF

Telephone: **01625 545700**
Facsimile: **01625 514510**

E-mail: **mail@dataprotection.gov.uk**
Website: **www.dataprotection.gov.uk**

CBI (2001). *CBI revised model draft clauses for use when transferring personal data to non-EEA countries*. Contact: **enquiry.desk@cbi.org.uk**

McKilligan, N, (2001) *Data protection – guide to data controller and data processor contracts*. DISC Data Protection Update Service Reference: **DISC PD 0012-6: 2001**.

USA Safe Harbor arrangements

The official site describing the US Safe Harbor arrangements is on:
http://www.export.gov/safeharbor/

Appendix A: Automated decisions

By written notice individuals can require a data controller to ensure that no decisions that significantly affect them are based solely on the processing by automatic means of personal data of which they are the subject.

Prospective, current and past employees have a right to know the logic of any automated decision making to which they are likely to be subject. Either a separate request can be made for which a fee of up to £10 can be charged, or if specifically stated the request can be included in a more general subject access request.

- Ensure that on request, promptly and in any event within 40 days, employees are provided with a statement of how any automated decision making process to which they are subject works. Include sufficient explanation for them to understand the range of factors taken into account and the way they are assessed without revealing 'trade secrets' of those who design or supply the systems *(Principle 6)*.

The Act limits the decision-making to which this provision applies to that based on an evaluation of matters relating to the individual. There are examples of matters that might be evaluated. These include the individual's performance at work, reliability and conduct.

The Act goes on to place obligations on a data controller where an automated decision is taken and no written notice has been received. It also sets out types of decisions where the data controller is exempt from these obligations and where a written notice, even if received, does not have effect. To qualify as an exempt decision certain conditions must be met.

Firstly:

- the decision must be taken in the course of steps taken;
  - for the purpose of considering whether to enter into a contract with the data subject;
  - with a view to entering into such a contract, or

- in the course of performing such a contract, or;
- the decision must be authorised or required by or under any enactment;

Secondly:

- the effect of the decision must be to grant a request of the data subject, or;
- steps must have been taken to safeguard the legitimate interests of the data subject (for example, by allowing them to make representations).

As the employer/employee relationship is a contractual one, automated decision taking in the context of this Code is likely to qualify as an exempt decision provided there are safeguards for an unsuccessful employee or potential employee such as a right of appeal or a right to make representations in some other meaningful way.

For example,

An employer places the educational qualifications of job applicants into categories and then enters these into a computer system which produces a score for each applicant. Only those applicants with a score of 25 or over are short listed. This is an automated decision but, provided safeguards are in place for those not short listed it is an exempt decision as it is taken for the purpose of considering whether to enter into a contract of employment with the applicant. Safeguards would be notifying applicants that an automated process is to be or has been used, giving them an opportunity to state why they should be considered separately and, if the case is valid, doing so.

For example,

An employer has a system that scans application forms. The employer asks applicants on the form what the minimum starting salary is they would accept. The system automatically rejects those applicants that put more than £50,000 per year. The decision falls outside the specific provisions on automated decision taking because it is not based on an evaluation of matters relating to the individual of the type referred to in the Act.

When individuals make subject access requests they are entitled to be told of the logic involved in any automated decision making that comes within the scope of the above provisions and affects or is likely to affect them. An employer is not obliged to provide this information in response to a wider subject access request unless it is specifically referred to in the request. If it is the subject of a separate request a separate fee can be charged.

Furthermore, an employer is not required to provide information in response that constitutes a trade secret. Neither the term 'logic' nor the term 'trade secret' is defined. The Commissioner takes the view that an employer is required to provide an explanation that enables the individual to understand the sorts of factors taken into account in the discussion and the way in which they are evaluated and translated into the decision. However, the employer is not required to give matters such as the precise weighting given to each factor which either the system supplier or the employer would reasonably want to keep secret from a competitor on the basis that it provides it with a significant competitive advantage.

Appendix B: Sensitive personal data

The conditions considered 'necessary' for the processing of sensitive personal data where the data subject has not give his/her explicit consent include those where:

(i) the processing is **necessary** for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment;

(ii) the processing:

a) is **necessary** for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings);

b) is **necessary** for the purpose of obtaining legal advice, or;

c) is otherwise **necessary** for the purposes of establishing, exercising or defending legal rights.

(iii) the processing is **necessary**:

a) for the administration of justice;

b) for the exercise of any functions conferred on any person by or under an enactment, or;

c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

(iv) the processing:

a) is of sensitive personal data consisting of information as to racial or ethnic origin;

b) is **necessary** for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and;

c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

(v) the processing:

a) is in the substantial public interest;

b) is **necessary** for the purposes of the prevention or detection of any unlawful act; and;

c) must necessarily be carried out without the explicit consent

of the data subject being sought so as not to prejudice those purposes.

(vi) the processing:

a) is of sensitive personal data consisting of information as to religious beliefs or other beliefs of a similar nature or physical or mental health or condition;

b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons:

(i) holding different religious or other beliefs or;

(ii) of different states of physical or mental health or condition, with a view to enabling such equality to be promoted or maintained;

c) does not support measures or decisions with respect to any particular data subject otherwise than with the explicit consent of that data subject; and;

d) does not cause nor is likely to cause, substantial damage or substantial distress to the data subject or any other person.