Grey Paper No. 8 – Data Protection

ESSENTIAL FACTS ABOUT DATA PROTECTION – THE DATA PROTECTION ACT 1998

The Data Protection Act 1998 came into force on 1 March 2000. The Act applies to all data processed since 24 October 1998.

Secondary legislation in relation to, amongst other things, notification procedures and fees has also come into force.

New legislation was required to implement the Data Protection Directive (95/46/EC) into United Kingdom Law.

MANUAL RECORDS

The Data Protection Act 1984 did not extend to the protection of data contained in manual records.

However, the Data Protection Act 1998 extends the definition of data to "information which ... is recorded as part of a relevant filing system or with the intention that it should form a part of a relevant filing system".

The term "relevant filing system" is defined as "any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible".

All personnel files will be covered by the new legislation. In addition, the phrase "by reference to criteria relating to individuals" would mean that a file of, for instance, disciplinary warnings or appraisals, would also be covered by the new legislation.

DEFINITIONS

Data controller means a person who determines the purposes for which and the manner in which any personal data are to be processed - i.e. the Theatre Company

Data processor means any person who processes data on behalf of the data controller - e.g. a Theatre company or an outsourced service provider

Data subject means an individual who is the subject of personal data – e.g. an employee, member, volunteer or customer.

THE DATA PROTECTION PRINCIPLES

The Data Protection Act 1998 refers to eight data protection principles, of which only the eighth was not to be found in the Data Protection Act 1984.

Personal data shall be

1. processed fairly and lawfully
2. obtained only for one or more specified or lawful purposes, and shall not be further processed in any manner incompatible with that purpose of those purposes
3. adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
4. accurate and, where necessary, kept up-to-date
5. not kept for longer than is necessary
6. processed in accordance with the rights of data subjects
7. protected by appropriate technical and organisational measures against unauthorised or unlawful processing, against accidental loss or damage
8. not transferred to a country or territory outside the European Economic Area unless that country or territory shows an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

All data controllers must comply with all the data protection principles irrespective of whether they are required to notify the Information Commissioner of processing operations.

PROCESSING PERSONAL DATA

Personal data shall not be processed unless one of certain conditions is met. Those conditions include

- The data subject has given his consent to the processing
- The processing is necessary either for the performance of a contract to which the data subject is a party or for the taking of steps and the request of the data subject with a view to entering into a contract (this would cover membership and audience related activities)
- The processing is necessary for compliance with any legal obligation to which the data controller (the person responsible for the processing) is subject other than an obligation imposed by contract
- The processing is necessary for the purposes of legitimate interest pursued by the data controller except where the data subject's fundamental rights prevail

PROCESSING OF SENSITIVE PERSONAL DATA

"Sensitive personal data" means personal data consisting of information as to

- the racial or ethnic origin of the data subject,
- his political opinions,
- his religious or other beliefs of a similar nature,
- whether he is a member of a Trade Union,
- his physical or mental health or condition,
- his sexual life,
- the commission or alleged commission by him of any offence, or
- any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings"

Such sensitive personal data will only be processed where, in addition to one or more of the above conditions being met, at least one of certain other conditions is also met.

Those additional conditions include

- the data subject has given his explicit consent to the processing of the personal data (more likely to be the case in relation to recruitment where an individual will usually have a free choice whether to apply for a particular job)
- 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
    - is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
    - is necessary for the purpose of obtaining legal advice, or
    - is otherwise necessary for the purposes of establishing, exercising or defending legal rights
    - is necessary for medical purposes
    - is necessary for ethnic monitoring purposes.

Where the Company is relying on a "necessary" condition, they should ensure that the decision making process is well documented.

RIGHTS OF ACCESS

Right of Access – at reasonable intervals, an individual has the right to be given (in hard copy) a description of all personal data held by the Company and the personal data itself, together with the purposes for which it is being processed, the recipients and the source of the personal data.

Automated Decisions – an individual has the right to be informed of the logic involved in decision taking where that decision is made solely by automated means, such as psychometric tests or credit checks. The logic need not be disclosed if it constitutes a trade secret.

Third Parties – there is no right of access where information would reveal the identity of a third party, unless either the consent of that third party is obtained, it is reasonable to proceed without consent (taking into account duties of confidentiality, attempts to obtain consent and express refusals to give consent) or the third party is a health professional who has compiled or contributed to a health record.

Nature of Request – all requests for access must be made in writing and the Company may charge a fee of up to £10. A data subject is entitled to a reply "promptly" and, in any event, within 40 days of receipt of:

- providing the information required to confirm the identity of the person making the request;
- providing the information required to locate the requested personal data; and
- the fee.

EXEMPTIONS TO THE RIGHT OF ACCESS

Confidential References – see separate section below.

Management Forecasts and Planning – where personal data is processed to assist the Company in the conduct of its business and subject access would be likely to prejudice the conduct of the business.

Negotiations – e.g. where subject access to information recording the intentions of the Company in negotiations with an employee would be likely to prejudice those negotiations.

Legal Professional Privilege – where data consists of information in respect of which such a claim could be maintained in legal proceedings.

OTHER RIGHTS

Preventing Processing - an individual may request in writing that the Company does not process personal data where such processing is likely to cause substantial damage or distress to him or another.

Automated Decisions – in addition to the above rights of access, no decision which significantly affects an individual may be based solely on the processing of personal data by automatic means unless the Company either is undertaking such processing in response to a request of the individual or allows the individual to appeal against such a decision.

ENFORCEMENT OF RIGHTS

Access - the court may order the Company to permit access by the individual to personal data.

Rectification, Blocking, Erasure and Destruction – the court may order the Company to take such action in relation to inaccurate data.

Compensation – the court may award compensation in respect of any breach of the new legislation which has resulted in loss or damage. Although under the new legislation, damages for distress will only be available where physical or economic damage has resulted, the European Commission has stated that damage should include psychological damage.

Complaint to the Information Commissioner – may lead to Enforcement or Information Notices.

NOTIFICATION

Data controllers are required to notify the Information Commissioner, before processing commences, of:

the nominated Data Protection Officer;

- a description of the personal data being or to be processed;
- the category of data subject to which they relate (e.g. employees);
- a description of the purpose or purposes for which the data are being or are to be processed;
- a description of any recipient to whom the data may be disclosed;

- those countries outside the EEA to which data is to be transferred;
- a general description of measures to be taken to comply with the seventh data protection principle.

The notification procedure will replace registration. Those with existing registrations will be sent a pre-printed form by the Information Commissioner to speed up notification.

It is not necessary to notify the Information Commissioner of processing which is for the purposes of appointments or removals, pay, discipline, superannuation, work management or other personnel matters.

STATISTICAL AND HISTORICAL RESEARCH

Where processing of personal data is carried out for the purposes of statistical or historical research and that data is not processed:

- to support measures or decisions with respect to particular individuals, and
- in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject,

such processing is not to be regarded as incompatible with the second principle and the personal data processed may be kept indefinitely, notwithstanding the fifth principle.

As long as the results of the research or any resulting statistics are not made available in a form which identifies data subjects, a data subject will not have those rights referred to as “Rights of Access” above.

OFFENCES

Notification related – failure to notify or acting outside notification.

Notice related – failure to comply with or making false statements in response to Enforcement or Information Notices.

Unlawful obtaining or disclosure of personal data.

Enforced subject access (not yet in force) – requiring the supply or production of a “relevant record” (criminal convictions, cautions etc) in connection with:

- the recruitment of another person as an employee,
- the continued employment of another person, or
- any contract for the provision of services by another person.

Personal liability of Directors, Managers, Secretaries or similar officers. On conviction, liable to a fine of up to £5,000.

SUGGESTIONS FOR COMPLIANCE – MANAGING DATA PROTECTION

CODE

- Establish a person responsible for Data Protection compliance, make line managers aware of the need for Data Protection compliance, make non-compliance a disciplinary offence and all audit policies and procedures for Data Protection compliance. [processed fairly and lawfully]
- CODE – Eliminate the collection of irrelevant or excessive personal data. [adequate, relevant and not excessive]

SUGGESTIONS FOR COMPLIANCE – RECORDS

CODE:

- Inform newly appointed staff or new customers what information will be kept about them, where it is obtained from, how it is used and to whom, if anyone, it will be disclosed. This might be done by means of a factsheet advising them of the above information and their right of access to their own personal data. [processed fairly and lawfully]
- Employees should be required to confirm their personal details annually and to notify changes of name, address, telephone number, bank and title to their personnel officer as soon as possible. [up

to date]

- Access to personal data held on computer should be restricted to named system users by password. Access to manual records holding individuals' personal data such as keys to filing cabinets should be similarly restricted. Managers should be advised not to keep personal data in insecure locations, such as desk drawers. [security]
- An individual's personal data should not be made available to other individuals in an employment context, other than to provide managers with information reasonably required in their management role. Include confidentiality clauses in contracts of employment which specifically refer to the use of other individuals' personal data. [security/management forecasts]
- The transmission of personal data by fax or email should only occur where the data may be received and held securely by the recipient. It is good practice to telephone the recipient prior to sending the personal data. This will ensure that a direct dial fax number is used where available or that the recipient does not have their email forwarded to a third party (such as when they are on holiday). Emailed personal data should be encrypted. A policy on the use of computers and telecommunications should deal with these security aspects. [security]
- Do not disclose details of an individual's sickness or other medical condition unless there is a legal obligation to do so or the individual has given explicit consent to the disclosure. In the employment context, do not make an individual's sickness or absence records available, unless needed by managers to perform their managerial role. [in accordance with rights]
- Do not use for general purposes personal data which has been specifically provided for the purposes of pension or insurance schemes or gained from such scheme administrators or trustees. [obtained for specified or lawful purposes]
- Ensure that all information obtained as a result of ethnic and other equal opportunities monitoring is kept in an anonymised form, unless there is a need to track individuals for specified reasons, say promotion, for which the individual's explicit consent will need to be obtained. [ethnic monitoring]
- Allow individuals to "opt out" of receiving marketing material from the organisation itself and any outside organisations. If any marketing exercise involves the use of details more personal than name and address only, a positive indication of consent would be required from the individual, such as by way of ticking an "opt in" box. [obtained for specified or lawful purposes]
- Do not disclose personal data to other organisations for the prevention or detection of fraud unless you are required by law to make the disclosure or you believe that failure to disclose, in a particular instance, is likely to prejudice the prevention or detection of crime. In any event, always double-check the identity of the other organisation before making any disclosure. [processed fairly and lawfully]
- Establish a system for promptly responding to subject access requests, including checking the identity of the individual making the request and obtaining any specific information necessary to respond to the request. Where an individual has requested information relating to personal data held about them, the Company should respond promptly to such a request and within an absolute maximum of 40 days. [access rights/in accordance with rights]
- Ensure that managers and other relevant people are aware of the nature of information which may be released to individuals following a subject access request. [adequate, relevant and not excessive]
- Confidential references – see separate section above.
- Establish a disclosure policy to deal with requests by third parties for an individual's personal data, including procedures for obtaining an individual's (explicit) consent, what to disclose in an emergency and verifying the identity of the third party. Depending upon whether accidental disclosure of the requested personal data to a third party would cause damage or distress to the data subject, verify identity by requesting a signature, witnessed signature, passport or personal data which would only be within the data subject's knowledge. [processed fairly and lawfully]
- Only publish information about individuals where there is either a legal obligation to do so (eg Companies House records) or the information is clearly not intrusive (eg marketing material).

[obtained for specified or lawful purposes]

- Ensure, wherever practicable, that information handed over to another organisation in connection with a prospective acquisition or merger situation is anonymised. Only disclose personal data after securing assurances (by means of a written confidentiality agreement) that it will only be used specifically for the evaluation of assets and liabilities, treated in confidence, not disclosed to third parties and destroyed after use. [processed fairly and lawfully/legitimate interest]
- Advise individuals, if possible, that their personal data are to be disclosed in connection with a prospective acquisition or merger and obtain their consent in relation to the disclosure of sensitive personal data. [processed fairly and lawfully]
- The Company should check that the records they hold as a result of a merger or acquisition are adequate, relevant, not excessive, accurate and up to date by checking information with individuals.
- Discipline and dismissal – see separate section above.
- When outsourcing data processing or disclosing personal data, the sender and recipient of personal data should enter into a written contract in which the recipient undertakes to keep the personal data confidential and to ensure that it is protected whilst in the recipient's hands. Although this is advisable where the sender and recipient are different organisations within the EEA, this is essential where personal data is being transferred outside the EEA (even if within the same group of organisations) [security/adequate level of protection]
- An employee's pay and personnel records (excluding pension documentation) might be deleted (from computer) or securely destroyed (if manually recorded) at the end of the seventh year following the year in which they leave. However, records kept for health and safety purposes may be retained for longer periods, if required, particularly in the case of those working with hazardous substances. [kept for no longer than necessary/security]

Ensure that any staff review or appraisal identifies the source of any comments, that the employee is shown any comments, given the opportunity to make observations or challenge any comments and that any observations or challenges are recorded as part of the official record. [adequate and accurate]

Where negotiations are taking place with an employee or customer in connection with, say, salary reviews or holiday complaint settlement respectively, it is not necessary to grant access to personal data which would show the intentions of the Company and would be likely to prejudice negotiations. [access rights/negotiations]

If a Company has taken legal advice in connection with proposed or actual legal proceedings by an individual, any such personal data would be covered by legal professional privilege and need not be disclosed. [access rights/privilege]

CCTV SURVEILLANCE

DRAFT CODE – Give both workers and others (such as customers and visitors) notification that video and/or audio monitoring is taking place by displaying prominent signs in the areas to be monitored, together with the reasons for that monitoring. It will rarely be possible to justify continuous monitoring or the use of both vide and audio monitoring together. [processed fairly and lawfully]

CCTV CODE - Cameras should be sited –

- If possible, in positions where only the intended area to be monitored is covered
- With the consent of adjacent occupiers if images are to be recorded of areas outside the intended area to be covered
- In areas where the public are made aware that they are entering an area covered by video surveillance.

CCTV CODE - Any sign should be clearly visible and legible to members of the public, for example

- A sign at the entrance of a building viewed from close up to warn of internal surveillance should be A4 size
- A sign in a car park viewed from inside a car to warn of external surveillance should be A3 size.

CCTV CODE - Any sign must contain the following information –

- The fact that surveillance is taking place (an image of a camera may be sufficient)
- The identity of the person or organisation responsible for the surveillance
- The purposes of the surveillance
- Details of whom to contact regarding the surveillance.

CCTV CODE - Such as –

- “Images are being monitored on behalf of ABC Limited for the purposes of crime prevention and your own security. Please contact XYZ Limited on 01273 456789 for further information.”

CCTV CODE - Recorded images should be –

- Used only for the purposes for which they were recorded
- Viewed in a restricted area
- Retained in a secure location
- Retained for longer than necessary and thereafter deleted.

DRAFT Theatre Policy on data Protection

1. INTRODUCTION

1.1. This Policy applies to all personal data held by the Company, whether it is held electronically or in hard copy. Electronically held data will include all data stored on an office computer, a home computer, a laptop computer, a personal organiser, mobile telephones or other similar equipment. Hard copy data will include all data held in filing cabinets, desks, notebooks or any other location. Personal data means any data relating to an individual, whether they are another member of staff, a customer, supplier or member of the public.

1.2. The [position] is responsible for ensuring that the Company complies with its obligations under the Data Protection Act 1998, together with any Codes of Practice issued by the Information Commissioner who provides guidance and enforces the Act.

1.3. All [management committee members] must read and comply with this Policy. In addition, the unlawful obtaining or disclosure of personal data in breach of the Act constitutes a criminal offence for which you may be personally liable for a fine of up to £5,000 if convicted.

2. RIGHT OF ACCESS

2.1. At reasonable intervals, an individual has the right to be given (in hard copy) a description of all personal data held, together with the purposes for which it is being processed, the recipients and the source of the personal data. There is no right of access where information would reveal the identity of a third party, unless either the consent of that third party is obtained or it is reasonable to proceed without consent (taking into account duties of confidentiality, attempts to obtain consent and express refusals to give consent).

2.2. The recipient of any request for disclosure personal data should forward the request to the [position] immediately as the Act requires a prompt response and, in any event, within 40 days of receipt. There are various exemptions to the right of access and these may apply in certain circumstances.

3. PERSONAL DATA HELD BY THE THEATRE COMPANY ABOUT YOU

3.1. The [Theatre] Company needs to keep and maintain records in respect of all employees, members, and it is therefore necessary to record, keep and process personal data relating to you. This data may be kept and maintained in computer and/or manual format. Please ensure that the [Theatre] Company is able to keep your own personal data up to date by notifying the [position] of any changes of name, address, telephone number, bank or other relevant personal information as soon as possible.

3.2. It may be necessary, in the course of the Company's duties and obligations as an employer, to disclose such data to third parties, including other employees, potential purchasers of the Company, potential investors, the Company's professional advisers, clients and potential clients and the Inland Revenue.

4. PERSONAL DATA HELD BY THE COMPANY ABOUT OTHERS

4.1. All personal data held on computer should be restricted to named system users by password. Access to manual records holding personal data should be similarly restricted to only those staff who require access. Staff must not keep personal data in insecure locations, such as desk drawers.

4.2. An individual's personal data should not be used for any purpose other than that for which it was obtained. It should therefore not be made available to third parties (including other employees), other than to provide managers with staff information reasonably required in their management role or where the consent of the individual has been obtained.

4.3. The transmission of personal data by fax or email should only occur where the data may be received and held securely by the recipient. It is good practice to telephone the recipient prior to sending the personal data. This will ensure that a direct dial fax number is used where available or that the recipient does not have their email forwarded to a third party (such as when they are on holiday). Emailed personal data should be encrypted.

4.4. Do not disclose details of an individual's sickness to third parties unless individual has given explicit consent to the disclosure. Any sick certificates should be sent directly to the [position].

4.5. If requested by the police or any other public body to disclose personal data, you must forward any such request to the [position] who will double-check the identity of the third party before making any disclosure.

4.6. If requested to give a corporate reference, pass any such request to the [position] who will double-check the identity of the third party and that the individual's consent has been given before providing any reference. On no account must you provide any information in a corporate capacity either orally or in writing in response to such a request. Any request by an individual to have access to a reference (whether given or received by the Company) must be referred to the [position].

4.7. Where a third party requests an individual's personal data, you must ensure that you have obtained the individual's (explicit) consent before disclosing any personal data (including home addresses and telephone numbers) in response to the request.

4.8. In an emergency, you must verify the identity of a third party by requesting a signature, witnessed signature, passport or personal data, as appropriate.

5. ACCEPTANCE

I confirm that I have read and understood the contents of this Policy

Signed: ……..

Name: ……..

Dated: ……..