

Collecting and using personal information

Briefing note for Association of British Orchestras

Author: Andrew Sharpe

Date: 10 March 2009

Contents

- Data Protection law
- Data protection obligations
- Compliance with the data protection principles
- Rights of individuals
- Using marketing lists

Data Protection Act 1998

An annotated and consolidated version of the Act is available online at:
<http://www.statutelaw.gov.uk/Home.aspx>

The Data Protection Act 1998 is the UK implementation of the European Union Data Protection Directive 95/46/EC. The Directive is available, together with most other European Union data protection materials, from the EU Commission data protection and privacy website run by the Director General Internal Market at:
http://europa.eu.int/comm/internal_market/privacy/index_en.htm

Role of Information Commissioner

The Information Commissioner is also responsible for enforcement of the Freedom of Information Act 2000 and Environmental Information Regulations 2004 in England & Wales and Northern Ireland. The Scottish Information Commissioner is only responsible for enforcement of the Freedom of Information (Scotland) Act 2002 and the Environmental Information (Scotland) Regulations 2004; he has no data protection responsibilities.



These notes give an overview of the law governing the processing of personal data in the UK, as these have to be understood to be able to process data for marketing and other standard commercial purposes.

The notes have been prepared for information purposes for the Association of British Orchestras and its members. Charles Russell LLP cannot accept any liability for any reliance placed upon these notes, and readers should obtain their own legal advice before acting upon any information set out in these notes.

1 Data Protection law

1.1 Data Protection Act 1998

The Data Protection Act 1998 (the "Act") introduced new data protection laws into the UK on 1 March 2000 and became fully in force, with a few minor exceptions, on 24 October 2001. The Act applies to any organisation that keeps records of the names of individuals, for example customers, suppliers or employees. The Act applies to data processing organisations in England and Wales, Northern Ireland and Scotland.

1.2 Data Protection Regulations

There are a number of Statutory Instruments that provide further data protection regulations, but these are also all available from the Statute Law website.

The most important of these is are Privacy and Electronic Communications (EC Directive) Regulations 2003 (the "Privacy Regulations") (as amended by the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2004). The Privacy Regulations implement the European Union Directive 2002/58/EC (the "Privacy Directive"), and concern the use of electronic communications for direct marketing – see below.

1.3 Information Commissioner's Legal Guidance

The Information Commissioner is the regulatory authority responsible for enforcing the Act. The Information Commissioner has published extensive legal guidance on the Act. This is available at:

http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf



2 Data Protection obligations

2.1 Processing

The Act regulates the processing of personal data by UK businesses, including manual records. The definition of processing includes virtually anything that can be done with personal information, including merely storing it or reading it on a computer screen. All processing of personal data must comply with the eight data protection principles shown below:

2.2 Personal data

The Act applies only to the processing of personal data, which is information from which a living individual can be identified, either by the information itself or by other data or information in the possession of the data controller.

It is possible to identify an individual without knowing the name and address of that particular individual, for instance by the recording of an individual by CCTV. The Information Commissioner considers any data capable of being processed by the data controller to enable the data controller to distinguish the data subject from any other individual as personal data. Most email addresses, as they identify a particular living individual, are therefore personal data.

Anonymous data that is obtained with the intention that it later be cross-referenced to a particular individual is also personal data. This is a particular feature of information obtained by tracking technology such as cookies. Even if there is no intention of linking the information to a name and address or e-mail address, but merely the desire to use the information to target that particular individual with advertising or to offer discounts or other services on a re-visit to a particular web site, such profile information is likely to be personal data.

Where personal identifiers are removed and destroyed from any data and only the information which has been stripped of all personal identifiers is retained, the retained information ceases to be personal data, provided that the data controller assesses that it is not likely that information will come into its possession to enable it to reconstitute the data.

Durant -v- Financial Services Authority [2003]

In Durant -v- Financial Services Authority the Court of Appeal gave guidance as to what amounts to "personal data" for the purposes of the Act. In summary, the Court held that records which make reference to an individual are not necessarily "personal data". Instead, the records must be relevant or proximate to the individual (i.e. significantly biographical or of which the individual was the focus of attention).

It is not sufficient that the records just relate to something in which the individual was involved. In addition, the records must contain "information that affects [the individual's] privacy, whether in his personal or family life, business or professional capacity".

Durant -v- Financial Services Authority [2003]

The Information Commissioner has published guidance on the Durant case (The 'Durant' Case and its impact on the interpretation of the Data Protection Act 1998' - 8 September 2004, available from the Information Commissioner's website at: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/the_durant_case_and_its_impact_on_the_interpretation_of_the_data_protection_act.pdf)

The full Court of Appeal judgement is available at: <http://www.hmcourts-service.gov.uk/judgmentsfiles/j2136/durant-v-fsa.htm>



The Information Commissioner has published guidance on the Durant case. In it he states:

“It may therefore be possible that the incidental inclusion of a name of an individual on a marketing list directed as business to business marketing will not have this privacy element to render the associated details with the name as personal data.

It is more likely that an individual’s name will be ‘personal data’ where the name appears together with other information about the named individual such as address, telephone number or information regarding his hobbies.

As such, marketing lists containing a name together with contact details such as address and/or telephone number and/or e-mail will be personal data.”

2.3 Data controllers

The Act applies to processing which is undertaken by data controllers. A data controller is defined as any person who determines the purposes for which and the manner in which personal data is, or is to be, processed. In other words virtually every business in the UK is a data controller. More than one organisation can be a data controller over the same personal data, and an organisation can be both a data controller over some of the personal data it holds and only a data processor of other personal data.

It is therefore important to note that subject to a concert goer being given the appropriate notice (see below), both an orchestra and a venue can be joint data controllers over the concert goers’ data.

2.4 The data protection principles

At the core of the Act are eight Data Protection Principles. These Data Protection Principles, derived from Article 6 of the Data Protection Directive, are set out at Schedule 1 Part 1 to the Act.

First Data Protection Principle

“Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-

- a) at least one of the conditions in Schedule 2 is met, and
- b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.”

Second Data Protection Principle

“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.”

Third Data Protection Principle

“Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.”



Fourth Data Protection Principle

“Personal data shall be accurate and, where necessary, kept up to date.”

Fifth Data Protection Principle

“Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.”

Sixth Data Protection Principle

“Personal data shall be processed in accordance with the rights of data subjects under this Act.”

Seventh Data Protection Principle

“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.”

Eighth Data Protection Principle

“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.”

3 Compliance with the data protection principles

3.1 Fair and lawful processing

To understand the First and Second Data Protection Principles it is necessary to understand the conditions in Schedule 2 and 3 of the Act.

The key condition at Schedule 2 is the data subject’s consent. The equivalent for sensitive personal data at Schedule 3 is explicit consent to the relevant processing.

Sensitive personal data is defined at section 2 of the Act – it is personal data relating to: racial or ethnic origin, political opinions, religious beliefs "or other beliefs of a similar nature", membership of a trade union, physical or mental health or condition, sexual life, information relating to the commission or alleged commission of any offence and information relating to criminal proceedings against the individual. For normal commercial data processing, it is unlikely that a data controller would need to process sensitive personal data. If sensitive personal data processing is required, special care ought to be taken over the relevant processes and internal procedures governing its use by the data controller.

Paragraph 6(1) of Schedule 2 states:

“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 by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.”



Most processing by businesses will either be with the consent of the individual or for its or a third party's legitimate interests, and so will be lawful under the Act.

Consent is always the preferred option. In most cases, therefore, the use of personal details should be described in a fair processing notice, with an opt-out (and/or opt-in for electronic communications) option either included or explained if the details are to be used for direct marketing (see below).

It is lawful to process information, including for direct marketing, from an individual whose details have been obtained from a third party, provided that the third party has obtained consent to the export of the individual's details for the relevant processing purposes. It is therefore possible for orchestras and venues to agree on data sharing mechanisms. There is no outright ban in the Act against such data sharing.

3.2 Obtaining data from the data subject

When obtaining personal data from an individual, for example by requesting the filling in of an online membership or application form, requesting users to register on a web site or taking customer details over the telephone, data controllers are required to make readily available to each individual certain information, including:

- the identity of the data controller;
- the purpose/s for which the data are to be processed, and
- other 'fairness' requirements such as the types of persons to whom the data are likely to be disclosed.

(See paragraph 2(1) and (3) of Part II to Schedule 1 of the Act). This information is often referred to as the "fair processing notice".

The Information Commissioner is currently consulting on a code of practice for such privacy notices – it would be prudent to ensure that any fair processing notice follows that draft code (available at:

http://www.ico.gov.uk/Home/about_us/consultations/our_consultations.aspx).

Where a data controller obtains personal data from someone other than the data subject to whom they relate, for example list rental or as a result of sharing between orchestra and venue, the data controller must also make readily available to individuals as soon as reasonably practicable a fair processing notice.

3.3 Exemption from fair processing notice

Data controllers can rely on an exemption from making available a fair processing notice where to do so "would involve a disproportionate effort" (Paragraph 3(2)(a) of Part 11 to Schedule 1 of the Act). There is little guidance on what "readily available" means in this context, or what is meant by "as soon as practicable".

"Disproportionate effort" is also not defined in the Act. The Information Commissioner has in his legal guidance stated that he will consider a number of factors in determining what is a disproportionate effort, including the nature of the data, the length of time and the cost involved to the data controller in providing the information.



The fact that the data controller has to expend a substantial amount of effort and/or cost in providing the information does not necessarily mean that the data controller can rely upon the disproportionate effort exemption.

3.4 Data retention

In order to follow best practice, each data controller should make a documented assessment of its business requirements for all personal data processing (as part of its data protection policy), which should state what the retention period or retention policy is for each type of personal data. Any retention periods which are proportionate to its properly assessed business reasons for keeping the personal data will be compliant with the Act.

3.5 Data security

A data controller will only be deemed to have complied with its obligation or not to be in breach of the Seventh Data Protection Principle if, having regard to the state of technological development and the cost of implementing any measures, its technical or organisational measures ensure a level of security appropriate to:

- the harm that might result from any unauthorised or unlawful processing or accidental loss, destruction or damage to the Personal Data ; and
- the nature of the Personal Data to be protected.

Where data controllers use third parties to carry out their data processing (i.e. subcontract or outsource any processing, for example to a printing or mailing house), then they remain liable for any unauthorised or unlawful processing of the data supplied to those third parties. Services agreements with the service providers must therefore include certain express provisions to control the use of the personal data, including minimum clauses:

- to ensure that the services provider is designated a “data processor” within the meaning of the Act;
- to state that the data processor cannot process the personal data supplied except within the terms of any instructions from the data controller; and
- to ensure that the data processor complies with the Seventh Data Protection Principle.

3.6 Transfers of Data out of Europe

This is a difficult area of the Act and specialist assistance should be sought if any such transfers are required. The Eight Data Protection Principle does not apply in a number of circumstances, the most important of which is where the consent of the data subject has been obtained for the transfer of data outside of the EEA. A statement to this effect should therefore be included in any fair processing notice.

4 Rights of individuals

The following sets out the main rights individuals have under the Act.



4.1 Data subject access requests

Data controllers have a duty under the Act to make certain information available at the individual's written request. A individual must now be informed, within 40 days of the request in most cases, of the following:

- the content of the personal data processed
- the purpose of the processing
- the recipients to whom the data may be disclosed, and
- the person or organisation from whom the data controller obtained the personal data.

Where a decision significantly affecting a individual is, or is likely to be, made about that individual by fully automated means, for the purpose of evaluating matters about that individual such as performance at work, creditworthiness, reliability or conduct, the individual is entitled to be told of the logic involved in the process. Only if this information constitutes a trade secret is the data controller permitted to withhold the logic.

A data controller may charge a fee for dealing with subject access. Currently, the maximum fee chargeable is £10, or £2 if it is a request for limited information from a credit reference agency. There are special rules that apply to fees for access to manual health records, where the maximum fee is currently £50, and education records, where there is a sliding scale ranging from £1 to £50 depending upon the number of pages to be provided.

There are exemptions to the duty to disclose information to the individual upon an access request. For example, there are special rules concerning the disclosure of health and education records.

4.2 Processing likely to cause damage or distress

If an individual considers that any particular processing of his or her personal data is or is likely to cause substantial damage or distress to that individual or another, then provided that damage or distress is or would be unwarranted, the individual can write to the data controller to demand that the relevant processing stop. A data controller in receipt of such a demand must respond within 21 days of receipt of the demand, stating reasons why any or all parts of the demand are to any extent unjustified. Individuals can then seek a court order to ensure compliance with the demand. These demands are currently extremely rare, with no public record of any court applications.

4.3 Requests for assessment

Individuals who believe themselves to be directly affected by personal data processing can request the Information Commissioner to investigate any processing undertaken by any data controller to determine whether or not it is carried out in compliance with the legislation. The Information Commissioner has no discretion to refuse a request for assessment and so this new procedure poses substantial risks for UK data controllers.



4.4 Direct Marketing

Section 11 of the Act states:

- “(1) An individual is entitled at any time by notice in writing to a data controller to require the data controller at the end of such period as is reasonable in the circumstances to cease, or not to begin, processing for the purposes of direct marketing personal data in respect of which he is the individual.*
- “(2) If the court is satisfied, on the application of any person who has given a notice under subsection (1), that the data controller has failed to comply with the notice, the court may order him to take such steps for complying with the notice as the court thinks fit.*
- “(3) In this section "direct marketing" means the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals.”*

There is no unequivocal guidance on how individuals should be informed of their right to prevent processing for marketing purposes. It is clear that the individual should be able to exercise his or her right without any undue conditions (for example, requiring delivery of notice by registered post) and without charge. Best practice is that as part of the fair processing note that should be included on any information gathering form there should be a statement describing the extent of direct marketing that will be undertaken, together with the relevant opt-out and/or opt-in questions, so that the individual is given the opportunity to exercise a section 11 right.

This does not prevent an organisation from collecting personal data with a fair processing notice stating that direct marketing will be undertaken unless the individual requests in writing that the marketing cease, with contact details on where to send the section 11 notice.

Direct Marketing Association

The Direct Marketing Association, states in its Direct Marketing Codes of Practice (3rd Edition) that an individual should be able to object to processing for marketing “with the minimum effort” (paragraph 5.21(b) of the Code, available from: <http://www.dma.org.uk/content/pro-code.asp>)

However, this practice may not be considered to be within the spirit of the Act as currently applied by organisations such as the members of the Direct Marketing Association. A data controller is permitted to maintain a list of individuals who have objected to the use of their details for direct marketing.

5 Using marketing lists

5.1 Electronic Communications Marketing (Regulation 22)

The Privacy Regulations state at Regulation 22(2):

“Except in the circumstances referred to in paragraph (3), a person shall neither transmit, nor instigate the transmission of, unsolicited communications for the purposes of direct marketing by means of electronic mail unless the recipient of the electronic mail has previously notified the sender that he consents for the time being to such communications being sent by, or at the instigation of, the sender.”



The Privacy Regulations therefore make it unlawful to send unsolicited e-mail or SMS without the prior consent of the individual subscriber recipient. Organisations wishing to use e-mail as part of their marketing strategy will therefore need to obtain opt-in consent from these individuals for use of their electronic communications contact details for direct marketing. At present only opt-out consent to all forms of direct marketing is required under the Act.

There are a number of important exceptions to this general “opt-in” rule. Although the Information Commissioner has advised that in general individuals’ email addresses are personal data, only direct marketing to “individual subscribers” is subject to the opt-in rule. The definition of “individual” in the Privacy Regulations relates to living individuals or unincorporated bodies comprising of living individuals (such as partnerships).

The definition of “subscriber” relates to the person having the contract with the communications provider for the supply of the relevant electronic communications service. It would therefore appear that individuals who work for limited companies or other incorporated bodies and have email addresses linked to their employers could be targeted for unsolicited electronic communications without their opt-in consent. Furthermore, generic email addresses could be subject to unsolicited communications without consent.

However, business recipients of spam can request that this direct marketing stop, as an “unsubscribe” address must be included in all electronic direct marketing (see below). As the Privacy Regulations do not relieve any person from their obligations under the Act, senders of spam would have to comply with a request where the direct marketing is directed at the relevant individual (section 11 of the Act).

This does leave open the question of what type of direct marketing may be caught by section 11; does this include direct marketing directed at a purchasing manager because of that manager’s role, for example, or marketing directed to generic email addresses? Unfortunately the guidance included with the Privacy Regulations does not make this clear.

Businesses will also be able to continue to market directly to individual subscribers with whom they have an “existing customer relationship” without obtaining opt-in consent. The Privacy Regulations broadly define an existing customer relationship in the terms used in the Privacy Directive that came before them, i.e. where the business obtains the individuals’ contact details in the course of a sale or negotiations for a sale of a product or service and is marketing its own similar products or services.

Businesses who wish to market their own similar products or services will therefore only need to:

- provide an e-mail direct marketing opt-out, which could be included in their current direct marketing opt-out clause on the form collecting the individuals’ contact details; and



- provide an “unsubscribe” facility to enable individuals to refuse further direct marketing.

Organisations will not be permitted under the Privacy Regulations to send direct marketing by electronic means if their identity is disguised or concealed on the communication or where the communication does not include a valid address to which the recipient may send a request to stop further direct marketing communications.

5.2 Telephone and Fax Marketing (Regulations 20 & 21)

No person may make an unsolicited telephone call or fax for the purposes of direct marketing where the relevant individual subscriber’s number is listed on the Fax Preference Service (“FPS”) of Telephone Preference Service (“TPS”) registers maintained by subsidiaries of the DMA for and on behalf of the Office of Communications (“Ofcom”) under the terms of the Privacy Regulations. In addition, direct marketing faxes cannot be made to “corporate subscribers” unless they have given their consent to receive such faxes. From 25 June 2004, corporate subscribers have been able to register their telephone numbers on the TPS, and thus prevent unsolicited direct marketing calls from being made to them, following the effective date of the amendment to the Privacy Regulations.

Organisations who intend to conduct telephone or fax direct marketing campaigns will therefore have to ensure that their contact details are “clean”, i.e. do not contain numbers on the relevant FPS or TPS registers. This can be done by an organisation itself, once it has obtained a licence from the FPS or TPS to use the relevant database to compare with its own contact details. Alternatively, the organisation can use a FPS or TPS licensee, as appropriate, as a marketing agent to conduct the marketing directly or to carry out list cleansing.

Organisations that conduct telephone or fax marketing may also wish to consider becoming associate members of the FPS or the TPS for reputation reasons. As an associate member, an organisation could demonstrate compliance with the Privacy Regulations by including the relevant logo on its marketing and other information, even where a marketing agency or list cleansing services provider is used. Currently an associate member’s fee for the FPS or the TPS is £250 per year.

5.3 Mail Marketing

Note that mail marketing is not subject to the same preference list checking obligations as telephone and fax marketing. However, the DMA’s Code of Practice (details above) requires its members to carry out similar list cleansing for mail direct marketing as for telephone and fax, using the Mail Preference Service.

FPS, TPS and MPS

The FPS and TPS licences are subject to fees, which can reach £2,320 per year for full licences. More information on FPS is available at: <http://www.tpsonline.org.uk/fps/> More information on TPS is available at: <http://www.tpsonline.org.uk/tps/> More information on MPS is available at <http://www.mpsonline.org.uk/mpsr/>.

More Information

Andrew Sharpe

+44 (0)20 7203 5194

andrew.sharpe@charlesrussell.co.uk