Data sharing in relation to the Data Protection Act

This four page guidance by **Roger Tomlinson** is based on the original "good practice" guide he wrote for the arts and entertainment industry, approved by the Information Commissioner, and followed through with Compliance Officers on the interpretation and implementation of the requirements of the Data Protection Act and the Privacy and Electronic Communications (EC Directive) Regulations. The **ADUK Data Ownership Guidelines** (co-authored with Tim Baker) updated this specifically for data sharing so that arts organisations could work together with their customer data for audience development. *This article does not constitute legal advice, but identifies acceptable good practice in 2014 for sharing data for the purposes of audience development in arts organisations.*

The Data Protection Acts 1984 and 1998 are frequently quoted as the reason data from customers of arts organisations cannot be shared. The application of the Acts and subsequent Regulations in 'custom and practice' does not support this view for most non-profit distributing charitable organisations, for the purposes of sharing data for audience development. However, there are restrictions in relation to out-bound telephone calls and SMS messaging.

Background

Firstly, the Acts do not confer 'ownership' of the customer data held by an organisation. **The members of the public 'own' their data**. An organisation has a **responsibility** to manage the data they retain and to control its use. In this latter respect the organisation is referred to as the Data Controller. Data Controllers can ensure the public are appropriately advised as to what will happen to their data, and can make appropriate contractual agreements to share data with related arts organisations provided they control the data usage. There are **no issues** in sharing "anonymised data" where the data does not identify individuals by name or address (postcodes can be shared) or provide any contact details.

Secondly, since 2003, internet communication methods have been covered by a different set of legislation: The Privacy and Electronic Communications (EC Directive) Regulations 2003. These establish that if a customer has a "transactional relationship" with an organisation, such as having purchased a ticket, then the organisation can **assume** they can contact the customer with information about similar events they are presenting. The key requirement is that any email

communication offers them an “unsubscribe” facility at the top of the message so they can opt out at any time.

Thirdly, the 2003 Regulations and the 1998 Act are predicated on the public being given appropriate notifications at the time of their data being captured about who is retaining their data, for what purpose, who it might be shared with and the results of any data processing. These notifications are therefore very important in terms of their communication to the public, not only on websites for online ticket purchase, but in print, etc. and for telephone and counter transactions. These notifications must state clearly, in a venue, that data will be shared for example with the visiting artist(s) or company that they are purchasing tickets for. The Compliance Officers at the Information Commissioner’s Office have regularly confirmed that this is good practice.

Fourthly, the implementation of the 1998 Act was the subject for much discussion at the time of its introduction, given that the legislation has some unusual legal features, with the interpretations of the Information Commissioner having considerable importance. The Act emphasises “good practice”, defined as:

1. Compliance with the enforceable provisions of the Act
2. Procedures which, although not themselves required by the Act, are designed to achieve compliance
3. Practice which goes beyond the enforceable requirements of the Act, but which the Commissioner considers to be desirable

The Arts Marketing Association and the Theatrical Management Association have also published, a “good practice” guide approved by the Information Commissioner. From the beginning this set out the permissions in order to share data. The application of the advice in the guide was modified when Compliance Officers agreed with “individual venue managers” that it was *“not unreasonable to assume continued interest in future productions of a similar nature at that venue".*

This meant that it was not necessary to obtain “informed consent” **during** the transaction, for contact by direct mail or email, provided there was appropriate notification to the customers and later offers of easy opt-out steps: *“Clear data protection notices should be placed at the point of data collection if an explicit explanation of this is not given to the data subject at the time of collection. This may be more problematic where data is collected over the telephone.”* Just to be clear, this change in practice came in 2002 and was advised to all Theatrical Management Association members. After the arrival of the 2003 Regulations, this simply aligns practice for direct mail with that of email and telephone data.

Good practice in data protection for audience development

There are many steps to achieve good practice in terms of capturing and managing customer data and controlling what happens to it, especially when data is to be shared. Note that this guidance largely excludes out-bound telephone calls and SMS messaging.

It is important to understand that there are advantages in terms of building relationships and engaging with people to ensure that they are happy with your data usage procedures. People who have willingly given permission are said to be more attentive to your communications and more responsive. The key point about data protection is that for most organisations and most customers it is only necessary to obtain "informed consent" once, the first time a person is entered into the database. Some organisations that utilise the "assumed consent" procedures below, follow up with either a mailed preference questionnaire or an emailed link to an on-line customer registration form, both to seek more information to profile the customer and to confirm their specific consent.

Below are 20 key points to "good practice" to enable data sharing:

1. Organisations must appoint a **Data Controller** and ensure that the person with that responsibility has a deputy to cover in their absence.

2. The Data Controller must be **trained in data protection procedures** and able to handle enquiries from colleagues and the public on an informed basis.

3. The Data Controller is responsible for ensuring that their colleagues are appropriately trained and briefed, and must **manage their data collection and data handling procedures**, monitoring any changes to the law and its interpretation.

4. Organisations must have a procedure for supplying an enquiring member of the public with **details of that person's customer record**, de-coding any category or similar information to make it comprehensible. There are time limits on responding to such requests and organisations can levy a limited charge for doing so.

5. Customer records must be **kept clean and up-to-date**, especially in terms of deceased individuals and gone-aways. There are service providers who can clean customer databases for this purpose. The data in customer records can be enhanced from ticketing history and transaction related behaviour and such data needs to be monitored for relevance and accuracy. "Personal data" is a legal definition and includes name and address, age and gender, and household information, and can be kept provided it is secure. Note that explicit permission is required to hold "sensitive data" (defined in the Act) such as ethnicity, sexual orientation, religion, political or trade union membership.

6. Customer records are usually kept on an **electronic database with appropriate security** to prevent non-authorised access so with password controlled access. Care should be taken

when making extractions that these cannot be copied on an unauthorised basis for example onto a USB memory stick.

7. The Data Controller must ensure that **full notification** is given to people whose data will be captured of:

    a. **who** is capturing their data (the legal name of the organisation),
    b. **what** they will use the data for ("sending information to keep you informed about the events and activities of our organisation"),
    c. **who** the data will be shared with ("visiting artist(s) and companies you book tickets to attend"), and
    d. **the outcome** of any data processing ("we will send you regular email newsletters and post you our brochure as well as information to keep you informed of latest events, activities and special offers").

8. Full notification must be **visible and accessible** (no 'small print'), in brochures, programmes at events, printed on the back of tickets if possible, on notices at the counter, in recorded messages before phone bookings, on web pages during the transaction – not requiring a 'click through' to be visible. **The assumption of consent can only apply to direct mail and email communications.**

9. The Data Controller must ensure that all direct mail and email communications with customers explain to them their **opt-out opportunities**, ideally with a freepost return address for direct mail and how to "unsubscribe" at the top of the message for email.

10. Opt-out must **not lead to the deletion of customer records** – instead these must have a 'flag' or other identifier on each record that they are not to be contacted. Some databases enable records to be supressed.

11. Beware when making customer record extractions for communication purposes to ensure that **opted-out or suppressed records are excluded**.

12. Extractions of customer records that have been used before for customer contact without complaint can be assumed to have consent for continued contact.

13. The Data Controller needs to draw up a simple **letter of agreement to form a contract** with each visiting artist(s) or company they need to share data with. The essence of this is to bind the organisation receiving the data to abide by the 1998 Act and the 2003 Regulations and only to use the data within the context of the notifications given to customers and their assumed consents. **This is essential and a legal requirement.**

14. The Data Controller is recommended to make such letters of agreement operate on the **"dual key"** principle in which any use of the data is advised at pre-determined notice (7 days suggested) of marketing communications using the data and both parties must consent to the use and the timing of the marketing action. This is not essential but is recommended.

15. Provided that customer records at a venue specifically relate to a particular visiting artist(s) or company then the **data can be shared with the visiting artist(s) or company** for the purpose of communications in relation to that same venue and visiting artist(s) or company. For communications purposes, extracted data sets for sharing should exclude all customers who have opted-out or been supressed.

16. Where the visiting artist(s) or company have received data from a venue they have performed at, it is not recommended to use this data for marketing events or activities at another venue unless the **originating venue has approved the marketing action** and ideally it is the venue issuing the communication for audience development purposes.

17. Where the visiting artist(s) or company wants to use the **shared data to compile a master list of their attenders** across multiple venues in order to circulate people with newsletters and touring date lists, it is necessary to obtain the permission of the originating venue(s) for this purpose.

18. In the circumstances in point 17, it is also recommended that either a **mailed preference questionnaire or an emailed link to an on-line customer registration form** is issued to people being added to a master list for the first time. This can be included in a first communication to customers.

19. Most direct mail and email **communications are personalised**, at the least addressed to named individuals, and have the potential to refer to previous events attended. This must be viewed from the point of the view of the individual customer. Will they understand how your organisation has their data? Will the reason you are communicating appear relevant to them?

20. It is important that if possible any **first contact is explained**: "Thank you for coming to see us at *AnyTown Theatre*, who have shared your contact information with us, so we can write to you about our other events and activities, our forthcoming programme and special offers we think you will be interested in. It is easy to opt-out or unsubscribe if you don't wish for us to contact you, etc." Such a first communication could include either a mailed preference questionnaire or an emailed link to an online customer registration form as well.

Finally, it is important to remember that data protection legislation must be viewed from the point of view of the people the law is intended to protect. Is their data safe with you? Most arts organisations want to build audiences and engage with people so that they can share with the public the benefits of arts engagement. If someone complains about being contacted, the arts organisation will apologise to them and desist from doing it again. Arts organisations do not set out to abuse customers or their personal data. By handling customer data under the "good practice" guidelines outlined above, you can comply with the spirit of the law and engage directly with people, respecting their information at the same time.

This article is made available under a Creative Commons license.