Data Protection in Tourism

by David Bowden
Jun 2008

Browse this article:

Summary

This article:

- sets out some of the basics for those involved in collecting and processing data in the tourism sector
- runs through some of the pitfalls
- highlights the hot topics that concern regulators or legislators in the field.

It introduces the main pieces of data protection legislation and outlines their requirements. It then goes on to focus on one of the eight data protection principles set out in the **Data Protection Act 1998**: that personal data shall be accurate and kept up to date. It examines the types of data currently held by tourism organisations, looks at relevant rulings, gives information on managing opt outs, data security and transfer. Finally it looks at how the system might change in the future, and gives some recommendations to those who deal with tourism data.

Introduction

It seems that hardly a day goes by without a headline story about the loss of personal data by a public organisation or business. Concern about this issue runs at an all-time high, as some of the publicised data breaches have involved sensitive data such as health records, National Insurance numbers, bank accounts and children.

Fortunately, the high-profile cases to date have not involved organisations in the travel and tourism sector. However there is no reason for complacency as it is not possible to predict where the next breach could occur.

Whilst businesses sometimes see data protection obligations as a hindrance and an example of the burdens placed on industry, it is important to remember that it is focused on the protection of the personal data and details of the individual. Good data management can enhance the relationship with customers, whereas inappropriate use can alienate the very people businesses want to reach. All the rules relate to the way names, addresses and further personal details should be collected, stored and used, and the information that should be provided to the individuals concerned.

This article sets out some of the basics for those involved in collecting and processing data in the tourism sector, runs through some of the pitfalls, and highlights the hot topics that concern

regulators or legislators in the field. Everyone involved in the collection and/or use of the information needs to be aware of the obligations. These include:

- individual employees
- owners of businesses
- data protection/management officers
- those collecting tourism data
- local authorities and other public bodies.

Liability may be incurred by individuals and by the organisations for which they work.

History of data protection rules

Article 8 of the 1950 European Convention on Human Rights provides that: "Everyone has the right to respect for his private and family life, his home and his correspondence" and that "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society".

Article 10 of this Convention also states that "Everyone has the right to freedom of expression. This right shall include freedom to …receive and impart information and ideas without interference by public authority and regardless of frontiers.

Data Protection Acts

In 1981, the Council of Europe (which now comprises 47 European countries) adopted a Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data. The UK gave effect to this when it enacted the **Data Protection Act 1984**.
As computers became smaller, more powerful, and cheaper, and were used to process ever-increasing amounts of data, often across traditional national boundaries, it was inevitable that further rules would follow. In 1995, the European Union adopted the Data Protection Directive. This Directive applies to all twenty-seven member states of the EU and covers not just data held on computers but also data held in conventional paper files. The UK gave effect to these new EU rules when it passed the **Data Protection Act 1998**, which is now fully in force and extends to non-computerised records created before 24 October 1998.
Further regulation followed from Brussels when in 2002 the EU adopted a Directive on E-Privacy which covers the use of cookies, email marketing and data used by power dialers. The UK brought this into force when it made the **Privacy and Electronic Communications (EC Directive) Regulations 2003** In addition to this, the basic standard elements of the different Acts have been used as a basis for a series of industry-led initiatives (such as the Mailing and Telephone Preference Services operated by the Direct Marketing Association (www.dma.org.uk) that help individuals manage the information held by others about them and the way they are used.

Data Protection Act 1998 overview

The Act distinguishes between personal and sensitive data. Sensitive data includes data about someone's health and ordinarily tourist organisations would not collect this sort of data. The Act says that to process personal data the data controller needs the data subject's consent – and that "explicit consent" is needed to process sensitive data. Obtaining and maintaining consent is always going to be a vital function for any organisation that collects personal data.

The Directive says that "unambiguous consent" is needed to process ordinary personal data. However, the UK government decided that ambiguous consent couldn't be consent and dropped the unambiguous requirement when it adopted the EU Directive. All that the UK requires is plain

"consent", but those who are processing data in other EU countries should be aware that the regime in other countries such as Italy and France is not as benign as the UK.

The Act also sets up a regulator, now called the Information Commissioner's Office (www.ico.gov.uk), to oversee the data protection rules in the UK. Tourist organisations processing personal data need to:

- register with the ICO
- pay the annual fee of £35
- notify ICO of the types of data they hold and the purposes for which they are processing it.

Some smaller bodies may escape this requirement if they fall within the small business exemption.

The ICO has over the years issued a large number of policy papers, guidance notes and has taken some enforcement action against companies that it does not believe are complying with the rules. It has not issued anything specific relating purely to the tourism sector.

Data protection principles

The Act says that there are eight data protection principles. These are as follows.

1. Fairly: personal data shall be processed fairly and lawfully.
2. Specified: personal data shall be obtained for one or more specified purposes.
3. Adequate: personal data shall be adequate, relevant and not excessive relating to the purposes for which they are processed.
4. Accurate: personal data shall be accurate and kept up to date.
5. Keeping: personal data shall not be kept for longer than is necessary.
6. Rights: personal data shall be processed in accordance with the data subject's rights.
7. Measures: appropriate technical measures shall be taken against unauthorised processing or accidental loss or destruction or damage to personal damage.
8. Transfers: personal data shall not be transferred outside Europe unless there is an adequate level of protection for data processing.

The focus in this article will be on the fourth principle about data quality and keeping data up to date. Other principles should not be overlooked – especially the seventh one about adequate technical measures to keep the data secure, the first one on fair processing and the fifth one, stating that personal data should not be kept for longer than is needed.

Data held by tourism bodies

Tourism South East

Taking Tourism South East (TSE) as an example, it has the following databases.

- A membership database with around 3000 records of its members, including information on name, address, email address and customer spend. At the moment this is not a full customer relationship database.
- A database that records key players in local authorities and MPs.
- A Programmes and Training Database, which may have indirect details of participant's ethnic origin (for example from their dietary requirements).

Some data is needed for reporting back to their Regional Development Agency (SEEDA) for funding purposes.

TSE would like to make more use of the consumer data it holds. Peter Colling, Development Services Director of TSE, feels it could analyse its consumer data better, conduct targeted marketing and could profile the data by using Arkenford profiles.

This is a product that has been developed by Arkenford Limited to segment consumers (for more details see www.arkenford.co.uk). It is a value-based segmentation that identifies the motivations and purchase drivers that influence people's leisure choices in tourism as well as in the activities they undertake. It includes data relating to restaurants, pubs and information on retail preference and media uptake.

Arkenford says that more than 150,000 UK residents have now been segmented using the system. With its corporate data, TSE would like to bring it all together in one place and at the same time, if budget permits, to rationalise it into a customer relationship database.

VisitBritain

VisitBritain has a Destination Management System (DMS) called EnglandNet, a database that manages all the information of interest to tourists to or within the UK. The DMS is used to collect data from the National Tourist Boards (Scotland, Northern Ireland, Wales, Channel Isles and Isle of Man) as well as from Regional Tourist Boards or sub-regions.

EnglandNet holds data on three different groups:

- accommodation – all assessed or rated: 42,000 providers
- attractions – 12,000
- events – 5,000.

EnglandNet gathers data from the following sources.

- From Data Stewards around the country (around 60 in total) who are responsible for collecting data for their region. For example, Kent Tourism Alliance can only update data records for Kent. Each data record has one owner – this is usually determined geographically, unless it has a national spread, such as Best Western.
- Quality in Tourism - QiT runs the assessed accommodation scheme for VisitBritain and sends through all its data to EnglandNet.
- Direct from businesses such as Premier Inn.

Most tourist organisations will also maintain a separate accounts database. EnglandNet, for example, holds no financial data at all.

EnglandNet data can be used by third parties to add to the data on their system. For example, in evidence to the Culture Media and Sport Select Committee of the House of Commons on 5th February 2008, Tom Wright CBE, the Chief Executive of VisitBritain said:

'EnglandNet does not just drive our websites, it drives a lot of the other key websites around the world, so EnglandNet is behind a lot of the content on Yell, for example, Google and TomTom®. All that content on EnglandNet is being brought onto satellite navigation systems so that when people drive through this country it tells them there is a great attraction off to the left here or there is a bed and breakfast off to the right here or there is a hotel.'

VisitBritain is presently looking at providing some of the data it holds to others, for example to train companies, which may want to know what assessed accommodation is near its stations.

Importance of consent

Unless a tourist organisation has the consent of the data subject to process the data, there is little it can do with it. The first data protection principle obliges all who collect and/or hold data to process it fairly. This, together with the second principle (processing for the purposes for which it was collected) means, in general, that data should never be used in a way that might come as a shock to the individual. It is good practice to get specific consent to use the data for the intended purpose.

For example, if data is collected in connection with a booking, obviously it is permitted to use and record the data for the purposes of processing that booking. It is also permitted to use the data to contact the individual about offers which are closely related to the services which the individual bought when the data was collected (eg hotel rates for the new season) unless the individual notifies the data collector that he or she does not wish to receive any further such communications.

It would not, however, be permitted to use the data to contact the consumer about entirely different products or services nor to pass their data to third parties (unless they are involved in providing the services which the customer is buying from the data collector). To use data in these "unrelated" ways requires the consent of the individuals.

The best time to obtain this consent is when the data is initially collected.

Consent in practice

Taking EnglandNet as an example, there is a consent structure in the database. Organisations listed on EnglandNet consent to VisitBritain contacting them for "other purposes". If an organisation told Heart of Kent, for example, that there was to be no data outsourcing or data transfers outside the European Economic Area (EEA), then these data preferences come over to VisitBritain.

Information Commissioner's rulings relevant to tourism

Neither the Information Commissioner's Office nor its predecessor (the Data Protection Registrar) has issued any specific sectorial guidance in the past relating to travel or tourism. The ICO has historically focused its attention on those business sectors where it receives the most complaints or queries or which are high-profile. Fortunately, to date tourism data has been underneath its radar.

There are two guidance notes that the ICO has issued in the past which are of relevance to those in the tourism sector. (Both are available at www.ico.gov.uk.)

1. *Stopping Unwanted Marketing Materials*. This has a template letter for data subjects to send if they want to prevent further direct marketing under section 11 of the Data Protection Act 1998. Those who manage data for tourism organisations will need to have a system in place to detect such requests and ensure that marketing preferences are updated when such communications are received.

2. *Sharing Personal Information: Our Approach*. This is aimed primarily at public bodies. It says that "Information sharing should be supported by a sound business case, preferably accompanied by a Privacy Impact Assessment. This should identify the intended benefits and demonstrate that the data protection risks have been identified and addressed."

The ICO also says that:

"*If organisations are going to share information they must have the capability and resources to ensure that its quality is good enough to support the use it will be put to.*

- *This might mean, for example, checking that information is up to date and recorded in a compatible format.*

- *Particular care is needed to avoid false matches, or making unfounded inferences.*
- *We expect measures to be taken to make sure inaccurate information is corrected by all organisations with which it has been shared.*
- *Where necessary we will take action to ensure that organisations involved in information-sharing pay due attention to information quality issues."*

Accuracy

It is important to ensure that data is accurate and up to date in accordance with the fourth data principle. Communications with individuals should always set out a convenient method of updating or correcting data held. Any requests to amend or delete data must be complied with unless there are reasonable grounds for believing that a particular request is fraudulent or misleading or that the person making the request is not the data subject. In any case, it is obviously good business/administrative practice to keep mailing lists and the like up to date.

Court rulings on data protection relevant to tourism

In **Source Informatics Limited [1999] EWCA Civ 3011**, the Court of Appeal considered sensitive data held by pharmacies about patient's prescriptions and what Source Informatics could do with this data by way of analysis of individual pharmacists dispensing habits. Although this would not appear to have much relevance to tourism, the court's comments on how widely data could be used if it is anonymised are of wider relevance to business.

The court took a very liberal approach and Lord Justice Simon Brown said: "*The concern of the law here is to protect the confider's personal privacy. That and that alone is the right at issue in this case. The patient has no proprietorial claim to the prescription form or to the information it contains. Of course he can bestow or withhold his custom as he pleases - the pharmacist, note, has no such right: he is by law bound to dispense to whoever presents a prescription. But that gives the patient no property in the information and no right to control its use provided only and always that his privacy is not put at risk.*"

Towards the end of the judgment he said this about data analysis and anonymised data: "*Thorough research and management depend in part upon the possibility of others checking that anonymised and aggregated information does correspond to the real world, by audit procedures which must inevitably involve checking identifiable cases. For present purposes, I say no more than that, provided, as I understand to be the case, the use of such identifiable data is very strictly controlled, there appears no reason to doubt that this is acceptable*"

Managing opt outs

Those involved in data management will need to cleanse any data they hold against the databases maintained by the Direct Marketing Association, which record data subject's data preferences. The immense practical scale of this task cannot be underestimated but is essential for tourism organisations in complying with their obligations under the fourth data protection principle on data quality.

At the moment, there are 14.8 million personal telephone numbers recorded on the Telephone Preference Service database. The owners of those numbers have opted not to receive telephone marketing call. There are also 1.3 million business telephone numbers (including direct dial corporate lines) recorded on the Corporate TPS database which records those business who have opted not to receive marketing telephone calls at work. The main Mailing Preference Service

database has 3.4 million records of business and personal addresses in the UK where data subjects have asked not to receive any more direct mail from any organisation.

Those undertaking email marketing may be able to take advantage of the "soft" opt-in exemption available under regulation 22 (3) of the **Privacy and Electronic Communications (EC Directive) Regulations 2003**. This allows marketing emails to be sent to prospects if:

- there has been a sale or negotiation for a sale
- the direct marketing is carried out by the same legal person who obtained the email address
- the direct marketing is limited to similar products and services, and
- the individual marketed was given an opportunity to opt out of marketing when their email address was first obtained.

Data security and transfer

Any organisation holding or processing personal data must ensure that they have appropriate security measures in place to ensure that the data cannot be accessed by unauthorised persons or organisations. The actual measures will depend to some extent on the nature of the organisation and its resources.

- In general, data should be stored in secure areas and not in public places or unsupervised places.
- Computers should have appropriate password protection and access to databases should be on a "need-to-know basis".
- Training should be given as to the importance of data security.
- If sensitive data is held, it will need to be appropriately encrypted.
- Unattended filing cabinets and computers should be locked.

The eighth data protection principle states that data should not be transferred outside the European Economic Area (EU plus Norway, Iceland and Liechtenstein) unless adequate levels of data protection are in place. There are some countries, including Switzerland and Australia, which the EU deems to have adequate equivalent legislation, but in practice, the easiest way of complying with the data protection legislation is to impose the EU "model terms" on the organisations to which you are transferring data.

Having these terms in a contract with the receiving parties means that the level of protection is automatically deemed to be adequate and if something goes wrong, there is a contractual right to redress.

What does the future hold?

At the moment, the ICO has put out for tender a research proposal for a review of the EU Data Protection Directive. The Directive was reviewed by the European Commission in 2003 when it decided to take no action. Under Article 33 of the Directive there must be a review every three years. The UK is trying to take the lead on this, partly out of frustration at the EU level. The present ICO initiated review will focus on 12 areas including:

- The potential for technology to safeguard personal privacy, for example through "privacy by design" approaches.
- How the law might better promote maximum accountability on the part of those handling personal information.
- How simplification and user-friendliness might be improved.

- How individuals' rights could be strengthened and updated.

Finally, an organisation called the Article 29 Working Party, which comprises the twenty-seven data protection authorities in each of the EU member states including the ICO in the UK, has published a twenty-nine page opinion on *Data Protection Issues Related to Search Engines* (WP 148). Those in tourism organisations who are looking at analysing or manipulating search engine data from Google or others as part of their data management strategy will need to familiarise themselves with this. Although it is stated to be an opinion, and is not put out for formal prior public consultation, documents from this working party have proved to carry great sway in the past with the European government.
Controversially, this opinion says that the consent of an individual website user must be obtained for all planned cross-relation of user data. It also says that search engines such as Google must clearly inform their website users upfront of the intended uses of their data.

Recommendations for tourism data holders

- Read the **guidance** for businesses and public bodies on the ICO website www.ico.gov.uk.
- Make sure your **registrations** are up to date and cover all the purposes for which you process data.
- Review your **collection policies** and **data protection statements** and make sure that they cover you for all the purposes for which you want/ need to process data.
- Make sure you have **processes for updating data** and are able to action quickly any requests to amend or delete data.
- Make sure you have systems and procedures in place to minimise the risk of **data falling into the wrong hands**.
- Ensure that all staff handling data are adequately **trained** and, in larger organisations, that there is a designated **data protection officer**.
- Make sure you can process any **data subject access requests** (individuals are entitled to be told, with certain exceptions, what data about them you hold and what it is used for).
- If you **transfer** any personal data outside the EEA, make sure that the model terms are included in your contract with the receiving party or that you have otherwise satisfied yourself that the data will be adequately protected.

About the author

David Bowden is a dual-qualified English and American lawyer and director of D Bowden Consulting Limited www.lobbyandlaw.com. It has been established for four years. David acts as a consultant to VisitBritain. If you need advice or assistance on resolving your domain name problems, he can be contacted at: info@lobbyandlaw.com or by telephone on (01462) 431444.