

DATA PROTECTION: THE DATA PROTECTION ACT

INTRODUCTION

The growth in the use of personal data has many benefits for businesses. However it's vital that those who collect and use personal data maintain the confidence of those who are asked to provide it by complying with the requirements of the Data Protection Act (DPA) 1998. It's therefore very important that you understand your obligations under the Act to ensure your practices are compliant and the information you obtain is stored securely.

THE LAW

The DPA applies to any business that's processing personal data.

Processing is a very broad term including obtaining and holding the data, as well as using and transmitting it. It's irrelevant whether these actions are manual or automated. The breadth of the DPA definition effectively means that from the moment of its collection to the moment that it's destroyed or fully anonymised, personal data is being processed and must thus be treated in accordance with the Act.

Personal data means data about identifiable living individuals. So if the data isn't about a living individual, the DPA doesn't apply. It also needs in most cases to be more than just a name. It's more likely that an individual's name will be personal data where the name appears together with other information about them, such as address or telephone number. The data also needs to relate to the individual rather than just being a mention of them.

The DPA works in two ways. It gives rights to individuals (known as data subjects) about whom information is held. It also places obligations on those (known as data controllers) who record and use personal information to do so in a way which follows the eight principles of good information handling (see below).

In order to comply with the DPA, you have a number of legal responsibilities:

- To notify the Information Commissioner you're processing information
- To process the personal information in accordance with the eight principles; and
- To respond to subject access requests received from individuals.

DATA PROTECTION: THE DATA PROTECTION ACT

NOTIFICATION

Anyone processing personal information must notify the Information Commissioner's Office (ICO) www.ico.gov.uk that they're doing so, unless their processing is exempt. Notification replaced the old system of Registration and most organisations will need to notify. There's a fee of £35, although no VAT is payable. Notifications are renewable annually and you'll usually be sent a reminder prior to its expiry.

There are some private companies that advertise to notify your business on your behalf. These companies have no official standing or powers under the Act. It is advisable that you do this yourself online at www.ico.gov.uk remembering that failure to notify is a criminal offence.

If you have a new purpose for holding or processing personal data it's vital you amend your notification.

THE EIGHT PRINCIPLES OF GOOD PRACTICE

The eight principles require that data must be:

- fairly and lawfully processed
- processed for limited purposes
- adequate, relevant and not excessive
- accurate and up to date
- not kept longer than necessary
- processed in accordance with the individual's rights
- secure
- not transferred to countries outside European Economic area unless the country has adequate protection for the individual

In addition, there are further provisions relating to the processing of sensitive data, which includes data on racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health, sex life, criminal proceedings or other convictions.

HOW TO COMPLY

There are a number of checks that you can make to ensure that you comply with the requirements of the DPA:

1. Your collection and use of personal information from clients must be fair and lawful. This normally means that, at the point you collect their personal details, you tell clients what the details will be used for and to whom they'll be passed. See Data Protection Policy section below.
2. You must take responsibility for all personal information held and used and ensure that appropriate security measures are in place to protect client information.
3. Your clients should be given the right to opt out of future marketing approaches at the time of information collection.
4. Your databases should be kept up to date and information should be held only as long as is necessary for the purposes for which it was collected.
5. Your clients must be given access, on request, to information held about them, and incorrect information must be amended or deleted without delay. Clients must be clearly informed of their rights in this respect.
6. You shouldn't seek to obtain information from persons under the age of 14 years without first securing parental consent.

DATA PROTECTION: THE DATA PROTECTION ACT

DATA PROTECTION POLICY

You need to have your own data protection policy, also known as a privacy policy, stating what the personal details you collect from clients will be used for and to whom they'll be passed. Clients must also be told of their right to see the information you hold on them.

ABTA can help you put together a data protection policy. There are examples at the end of this guidance note. Your policy must be available to your clients and must feature in your brochure and on your website. We can also provide data protection notices for you to display in your offices.

SUBJECT ACCESS REQUESTS

Sections 7, 8 and 9 of the Act give individuals a general right of access to the personal data you hold which relates to them. Generally the information you hold will be information you can disclose having taken into consideration any exemptions that apply. Exemptions apply to data processed for statutory functions relating to areas of crime and taxation. Other exemptions include confidential references you give although this doesn't apply to references you receive.

You have 40 days to comply with a request and you may charge a fee of up to £10. For further guidance on how to deal with subject access requests, visit www.ico.gov.uk.

MARKETING

If you wish to use unsolicited electronic marketing communications for purposes such as product development and the solicitation of potential customers, you need to be aware of the UK Privacy and Electronic Communications (EC Directive) Regulations 2003. These provide that:

- unsolicited marketing faxes mustn't be sent to individual subscribers without their prior consent;
- individual subscribers have a statutory right to opt out of unsolicited telephone marketing either by telling the caller or by registration on a central stop list;
- corporate subscribers can't opt out of telephone sales but have the right to opt out of unsolicited marketing faxes;
- automated calling systems must have the prior consent of both corporate and individual subscribers; and
- unsolicited emails or SMS can't be sent to any individual who hasn't consented unless the email or phone number was collected in the context of a commercial relationship.

For further information, see our guidance note *Data Protection: Privacy & Marketing Law*.

THIRD PARTIES

You may receive requests from third parties for information you hold about individuals. Examples include suppliers, employee references, solicitors, and the police.

In these circumstances you should only release information where the third party is able to satisfy you that the data subject has given his or her specific approval or where the data subject has already given, or is readily available to give, consent. Consent will normally have been obtained during the booking process.

DATA PROTECTION: THE DATA PROTECTION ACT

Contrary to popular belief, the police must also comply fully with the principles of the Act. They'll normally use an exemption of the Act which exists for the Detection of Crime or the Apprehension or Prosecution of Offenders, to request information.

Companies must also be careful when providing information that involves a third party. Unless you have the explicit permission of a third party to pass on data to the requester, you must black out that information, while providing as full a disclosure as you can to the person who made the request.

HOW LONG SHOULD YOU KEEP DATA

It mustn't be kept any longer than necessary so you need to formulate your own retention policy. If possible, you should keep files for six years, as that's the length of time within which a client may bring a legal claim. However, more sensitive data, such as credit card details, shouldn't be kept for this long but should be destroyed after they've been used for the purpose for which they were given.

This document is intended as a guide only and can't be a substitute for specific advice.

© ABTA Ltd

DATA PROTECTION

Contents

- Data Protection wording for travel agents (model)
- Data Protection wording for tour operators (model)
- Data Protection best practice for telesales

Please note that these models are intended as a guide only and can't be a substitute for specific legal advice. ABTA will not be responsible for any loss suffered as a result of reliance on this document.

Your booking

In order to process your booking and to ensure that your travel arrangements run smoothly and meet your requirements we need to use the information you provide such as name, address, any special needs/dietary requirements etc.

We take full responsibility for ensuring that proper security measures are in place to protect your information. We must pass the information on to the relevant suppliers of your travel arrangements such as your tour operator, airlines, hotels, transport companies etc. The information may also be provided to security or credit checking companies, public authorities such as customs/immigration if required by them, or as required by law.

Additionally, where your holiday is outside the European Economic Area (EEA), controls on data protection in your destination may not be as strong as the legal requirements in this country. We will not however, pass any information onto any person not responsible for part of your travel arrangements. This applies to any sensitive information that you give to us such as details of any disabilities, or dietary/religious requirements. **(If we cannot pass this information to the relevant suppliers, whether in the EEA or not, we cannot provide your booking. In making this booking, you consent to this information being passed on to the relevant persons.)**

Usually your tour operator or other principal will pass this information onto their suppliers once we have provided it to them. The tour operator or other principal's use of your information is subject to their policy, both in respect of your booking and any future marketing, and is their responsibility. Please ask either us or them for a copy of this if you would like to see it.

Your data controller is: *[insert the name of business or individual]*

You are entitled to a copy of your information held by us. If you would like to see this please ask us. [We may make a small charge for providing this to you].

Marketing

**[optional paragraph: we will not use your information for any purpose other than carrying out your booking.]

**[optional paragraph: we will hold your information, where collected by us, and may use it to inform you of offers in the future. If you do not wish to receive such approaches in the future, please tick this box

**[optional paragraph: We may also provide your details to selected third parties for similar purposes. If you do not wish to receive such approaches in the future, please tick this box

* Delete as appropriate

Statement for booking form, checklist or website: "I have understood and consent to the terms set out in the data protection policy." Please tick this box

Your booking

In order to process your booking and to ensure that your travel arrangements run smoothly and meet your requirements we *[and your travel agent] need to use the information you provide such as name, address, any special needs/dietary requirements etc.

We take full responsibility for ensuring that proper security measures are in place to protect your information. We must pass the information on to the relevant suppliers of your travel arrangements such as airlines, hotels, transport companies etc. The information may also be provided to security or credit checking companies, public authorities such as customs/immigration if required by them, or as required by law.

Additionally, where your holiday is outside the European Economic Area (EEA), controls on data protection in your destination may not be as strong as the legal requirements in this country. We will not however, pass any information onto any person not responsible for part of your travel arrangements. This applies to any sensitive information that you give to us such as details of any disabilities, or dietary/religious requirements. **(If we cannot pass this information to the relevant suppliers, whether in the EEA or not, we cannot provide your booking. In making this booking, you consent to this information being passed on to the relevant persons.)**

**[optional paragraph: Please note that where information is also held by your travel agent, this is subject to your agents own data protection policy.]

Your data controller is: *[insert the name of business or individual]*

You are entitled to a copy of your information held by us. If you would like to see this please contact [the data controller named above] [us]
[We may make a small charge for providing this to you].

Marketing:

**[optional paragraph: we will not use your information for any purpose other than carrying out your booking.]

**[optional paragraph: we will hold your information, where collected by us, and may use it to inform you of offers in the future or to send you brochures. If you do not wish to receive such approaches in the future, please tick this box

**[optional paragraph: We may also provide your details to selected third parties for similar purposes. If you do not wish to receive such approaches in the future, please tick this box

* Delete as appropriate

Statement for booking form, checklist or website:

"I have understood and consent to the terms set out in the data protection policy." Please tick this box

1. Staff at point of sale should be informed of the requirements of the Data Protection Act 1998 and be able to answer basic questions relating to the data protection policy of the business. In this respect, staff should have received a copy of this policy.
2. Staff at point of sale should be able to deal with requests for access to data and to pass them onto the correct individual within the organisation or to inform the consumer of the requirements necessary in order to obtain copies of the information held about them.
3. Before a booking is completed, staff should provide basic details regarding data protection to the client and a suggested wording is set out below:-

We take full responsibility for ensuring that proper security measures are in place to protect your information. When you make a booking, you consent to all the information you provide to being passed on to your suppliers, wherever they may be based.

Details of our data protection policy will be sent out with our documentation. Please read this carefully.