Outsourcing

A guide for small and medium-sized businesses

Data Protection Act

The Data Protection Act 1998 (DPA) is based around eight principles of 'good information handling'. These give people specific rights in relation to their personal information and place certain obligations on those organisations that are responsible for processing it.

An overview of the main provisions of DPA can be found in The Guide to Data Protection. This is part of a series of guidance, which goes into more detail than the Guide to DPA, to help you to fully understand your obligations, as well as promoting good practice.

This guidance explains the factors to be considered when choosing to use another organisation (whether inside or outside the EEA) to process personal data on your behalf.

Overview

As a data controller you may wish to use another organisation to process personal data on your behalf. If you decide to outsource your data processing to another organisation the DPA imposes certain restrictions and obligations on you in relation to that processing, as set out below.

An organisation that processes personal data is required to handle personal data in accordance with the data protection principles. A data controller may choose to use another organisation to process personal data on its behalf – a data processor.

The data controller remains responsible for ensuring its processing complies with the DPA, whether it processes in-house or engages a data processor.

Where a data processor is used the data controller must ensure that suitable security arrangements are in place in order to comply with

the seventh data protection principle.

If a data processor is located outside the EEA, the data controller must ensure that any transfer of personal data to the processor complies with the requirements of the eighth data protection principle.

What the DPA says

The seventh data protection principle provides that:

"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".

Where a data controller chooses to use a data processor, paragraphs 11 & 12 of Schedule 1 of the DPA introduce additional obligations on the data controller as follows:

"11.
Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller must in order to comply with the seventh principle –

(a) choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and

(b) take reasonable steps to ensure compliance with those measures".

"12.
Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller is not to be regarded as complying with the seventh principle unless –

(a) the processing is carried out under a contract –
  (i) which is made or evidenced in writing, and
  (ii) under which the data processor is to act only on instructions from the data controller, and

(b) the contract requires the data processor to comply with obligations equivalent to those imposed on a data controller by the seventh principle".

The eighth data protection principle provides that:

"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"

(Part 1 of Schedule 1 to the DPA).

Security Measures and outsourcing

The Seventh Data Protection Principle requires you to take appropriate technical and organisational measures to protect the personal data you process, whether you process it yourself or whether someone else (in the UK or overseas) does it for you.

In deciding what security measures are appropriate, you need to take into account the sort of personal data you are dealing with, the harm that might result from its misuse, the technology that is available to protect the data and the cost of ensuring appropriate security for the data.

If you decide to use another organisation to process personal data for you, you will remain legally responsible for the security of the data and for protecting the rights of the individuals whose data is being processed (the data subjects).

The DPA requires you to ensure that you chose a data processor that you consider will be capable of carrying out the processing in a secure manner. In addition, while they are working for you, you

should have in place arrangements (such as regular reports or inspections) to allow you to check that your chosen processor is processing the data in an appropriate manner. Remember, although you may be passing the job of processing to another organisation, you will continue to be responsible to both the Information Commissioner and the data subjects for the security of the data and the protection of the data subjects' rights.

The DPA requires you to have a written contract with your chosen processor. The contract must ensure that the processor:

- may only use and disclose the personal data in accordance with your instructions; and
- must take appropriate security measures to protect the data.

International outsourcing

You may wish to use another business located outside the UK to process personal data on your behalf. If you decide to outsource your data processing to a data processor located outside the European Economic Area (the EEA), the arrangement will involve the transfer of personal data falling within the restriction contained in the Eighth Data Protection Principle.

The Eighth Principle prohibits the transfer of personal data from the UK to a country outside the EEA unless that country (the third country) ensures an adequate level of protection for the rights and freedoms of the individuals (data subjects) whose data is being transferred. Therefore, if you transfer personal data, for example, to a call centre based in Asia or a processor based in the USA, you will need to ensure that your data subjects' rights are adequately protected.

If you transfer personal data to a data processor in a third country you will remain subject to the Information Commissioner's powers of enforcement and will continue to be responsible for protecting the data subjects' in relation to the overseas processing of their personal data by your chosen data processor.

Means of ensuring adequate protection for the rights of data subjects in international outsourcing

Model Contract Clauses

One means of ensuring adequate protection is the use of European Commission-approved Model Contract Clauses. The clauses tailored for transfers outside the EEA from data controller to data processor

have been approved by the European Commission and the Information Commissioner as offering adequate safeguards for the protection of the rights and freedoms of data subjects in connection with international transfers of data.

The clauses are in a standard form which may not be amended. They may however be incorporated in their entirety into your data processing service agreement with your overseas data processor. By incorporating the clauses in their entirely you will ensure adequate safeguards for the rights of the data subjects provided that nothing in the rest of the agreement changes the effect of the clauses.

Using model contract terms will satisfy the requirement (in the Seventh principle) for a written security contract and will fall within an exception to restriction on international data transfers set out in the Eighth Principle. For these reasons model contract clauses are often used in international outsourcing arrangements.

For more information on the model clauses see the ICO Guidance Sending personal data outside the European Economic Area web page and the detailed guidance on model contract clauses.

Other means

You do not necessarily need to use the model contract clauses when entering into an international outsourcing arrangement if you have found an alternative means of complying with, or using an exception to, the Eighth Principle. For example, ensuring compliance with the security requirements of the Seventh Principle will go some way towards satisfying the adequacy requirements of the Eighth Principle (given the continuing contractual relationship between you and your processor and your continuing liability for data protection compliance under the Act).

For further information about compliance with the Eighth Principle and exceptions to the Eighth principle see the ICO Guidance Sending personal data outside the European Economic Area web page and the detailed guidance on Assessing adequacy of protection for the rights of data subjects.

International sub-processing arrangements

If you choose to use a UK organisation to process personal data on your behalf, your UK data processor may suggest that it may

advantageous to you both if it subcontracts the processing to an organisation located outside the EEA.

As data controller you will remain liable for compliance with the DPA in relation to both the processing and any sub-processing (whether that processing is carried out in the UK or overseas). It is therefore important that you are satisfied that the proposed subcontracting will not materially increase the security risks to the data being processed nor adversely affect the rights of the data subjects.

Where the sub-processing arrangements will result in personal data being transferred outside the EEA, you must also ensure that any proposed transfer of personal data complies with, or falls within an exception to, the Eighth Principle prohibition on the international transfer of personal data. As data controller you must expressly authorise any international subcontracting. The data processor cannot choose to enter into sub-processing arrangements without your approval.

Non-EEA Processor and non-EEA Sub-processor

If you are outsourcing your data processing to an organisation outside the EEA the Eighth Principle issues will already have been addressed in the initial outsourcing arrangements between you and your overseas processor.

If your overseas processor proposes sub-contracting the processing to another overseas business he cannot do so without your prior approval. Given that you will remain responsible for protecting the rights of the data subjects (whether the processing is carried out by you, your processor or a sub-processor) you will need to ensure that appropriate contractual arrangements are in place to protect your position and seek redress from any party (the processor or sub-processor) that is in breach of its data processing obligations.

This is perhaps most simply achieved by inserting an additional clause into the controller to processor model contract clauses. If you approve the proposed sub-contracting you should also ensure that the controller to processor model contract clauses include additional obligations on the processor to:

- contract with the sub-processor on the same terms (particularly with regard to security arrangements) as set out in the main controller to processor agreement; and
- enforce the terms of the sub-processing contract against the sub-processor should there be any breach of its terms.

Any contract between your processor and the sub-processor should therefore mirror the main contract between you and your processor.

The Commission-Approved Controller to Processor contract clauses allow for the possibility of your non-EEA processor wishing to use a sub-processor. These clauses may therefore provide an appropriate means of addressing your Eighth Principle obligations where you are using a non-EEA processor.

UK Processor and non-EEA Sub-processor

Where your contract with your processor envisaged all processing being carried out in the UK, if it later agreed that some sub-processing is to be carried out outside the EEA, you will need to amend your controller/processor service contract. The contract will need to be amended firstly, to authorise the sub-processing and secondly, to address how the Eighth Principle is to be complied with in relation to the transfer of personal data to the sub-processor outside the EEA.

You should remember that the model contract clauses only deal with international transfers of personal data from data controllers to either other data controllers or to data processors. The model contract clauses do not cover transfers by data processors in the EEA to sub-processors outside the EEA. Therefore, any proposed sub-processing by your UK processor involving a transfer of data outside the EEA will need to use a means other than the model contract clauses to satisfy, or be exempted from, the requirements of the Eighth Principle.

General points on international outsourcing

Before using a non-EEA based data processor you should consider whether there is any particular legislation in place in the country or territory where your chosen processor is located which might adversely affect the rights of the data subjects whose data is to be transferred.

If particular legislation gives rise to concern, as part of your assessment as to the adequacy of the protection available for the rights of the data subjects, you will need to consider any risks the legislation may pose, the likelihood of you or your processor being subject to that legislation and how you will respond if required to do so under that legislation.

Where, in the light of the above considerations, foreign legislation poses unacceptable risks to the rights of data subjects you may not

be able to transfer personal data to that country unless you can identify and use an exception to the Eighth Principle (such as the model contract clauses). Even if you are able to transfer data in reliance upon an exception, you should have procedures and measures in place to deal with any requests for information that you or your processor may receive under legislation in the country in which your processor is located.

If you or your data processor receives a request for information from another jurisdiction, you will need to decide whether you are able to comply with the request. If you decide to comply it is good practice to ask for more information from the requesting authority to ensure that the request is specific enough to allow you to be able to identify, retrieve and transfer only that information that is relevant and necessary to comply with the request.

Good practice recommendations

The following good practice recommendations may be helpful if you decide to use an organisation to process data on your behalf:

- Select a reputable organisation offering suitable guarantees as to their ability to ensure the security of personal data.
- Ensure the organisation has appropriate data security measures in place.
- Ensure your processor makes and has made appropriate security checks on its staff.
- Ensure that you are able to transfer personal data to a non-EEA processor in compliance with, or in reliance upon an exception to, the Eighth Data Protection Principle.
- Ensure the contract with your processor is enforceable in the UK (and if your processor is located in another jurisdiction, the jurisdiction of the processor).
- Require your processor to report any security breaches or other problems (including requests for personal data from other jurisdictions).
- Have procedures in place to allow you to act appropriately on receipt of security or problem reports from your processor.

Other considerations

Further guidance on international transfer arrangements is available:

- Making your own assessment of the adequacy of the level of protection for the rights of data subjects

- Using Standard Contractual Terms (Model Contract Clauses)
- Binding Corporate Rules

More information

This guidance will be reviewed and considered from time to time in line with new decisions of the Information Commissioner, Tribunals and courts.

It is a guide to our general recommended approach, although individual cases will always be decided on the basis of their particular circumstances.

If you need any more information about this or any other aspect of freedom of information or data protection, please Contact us: see our website www.ico.org.uk.