Outsourcing the processing of personal data

information commissioner
Barrantagh Fysseree

This advice note sets out what you need to do to comply with the Data Protection Act 2002 (DPA) when you outsource the processing of personal information. Typical examples would include outsourcing your payroll function or customer mailings. It sets out which parts of the DPA are important when outsourcing and provides some good practice recommendations.

It applies when you use another organisation (a 'data processor') to process personal information for you, even though you keep liability for the information and full control over its use.

What does the DPA require?
When you contract or arrange with someone to process personal information on your behalf you remain responsible for the processing. This means that you will be liable for breaches of the DPA.

Outsourcing to <u>any</u> organisation
The DPA requires you to take appropriate technical and organisational measures to protect the personal information you process, whether you process it yourself or whether someone else does it for you.

To decide what measures are appropriate you need to take into account the sort of information you have, the harm that might result from its misuse, the technology that is available to protect the information and also what it would cost to ensure an appropriate level of security.

When you employ another organisation to process personal information for you, you must choose one that you consider can carry out the work in a secure manner and, while the work is going on, you should check that they are doing this.

You must also have a written contract in place with them. This contract must:
- make sure they only use and disclose the personal data in line with your instructions; and
- require them to take appropriate security measures.

The contract must be in place regardless of where the data processor is based.

Outsourcing to an organisation outside the EEA
The DPA, specifically the Eighth Data Protection Principle, requires that where personal information is transferred to any country or territory outside the European Economic Area there should be an adequate level of protection in place.

If you outsource work on personal information to an organisation outside the EEA, for example, to a call centre based in Asia or a processor based in the USA, you will have to make sure that the information is adequately protected. This will apply to the method you use to transfer the information to and from the processor, as well as to the work itself.

There are two relatively simple ways to do this.

- If you use an organisation based outside the EEA to act on your behalf, as long as there are appropriate security measures in place, it is likely that there will be adequate protection for personal information. This is because the use of appropriate security measures, the selection

of a reputable organisation and restrictions on the use of the information will all help ensure an appropriate level of protection for personal data. **However, you need to be sure that the contract with the other organisation and its terms are enforceable in the country in which the processor is located.**

- You can also use the model contract clauses approved by the European Commission for transfers to organisations outside the EEA acting on your behalf. These contract terms can be used independently or incorporated into your main contract for services with the organisation. These terms can be found on the European Union website at: eur-lex.europa.eu/LexUriServ/site/en/oj/2002/l_006/l_00620020110en00520062.pdf

These are only two of the ways of ensuring adequate protection for the information you transfer to your processor. Other ways exist depending on the particular circumstances of the transfer and more information can be obtained from the Information Commissioner.

Seventh Data Protection Principle - appropriate security measures
What is meant by 'appropriate security measures' will depend on all the circumstances of the transfer. You should consider the type of information, potential harm and available technology.

Where the transfer is to outside the EEA you should also consider the particular security risks associated with the recipient country, the existence of any data protection legislation in that country, or any other legislation which may affect the security of the data.

As part of your assessment as to the adequacy of the protection available for the information being transferred you will need to consider other legislation, any risks this may pose, the likelihood of you or your processor being subject to that legislation and how you will respond if necessary.

Sixth Data Protection Principle - Complying with subject access requests
You will need to make sure you have procedures and measures in place to deal with any subject access requests you or your processor may receive under legislation in the country in which the processor is located. If either you or your processor receives a request for information from another jurisdiction, you will need to decide whether or not you are able to comply with the request.

GOOD PRACTICE RECOMMENDATIONS

- Select a reputable organisation offering suitable guarantees about their ability to ensure the security of personal data.
- Make sure the contract with the organisation is enforceable both in the UK and in the country in which the organisation is located.
- Make sure the organisation has appropriate security measures in place.
- Make sure that they make appropriate checks on their staff.
- Audit the other organisation regularly to make sure they are 'up to scratch'.
- Require the organisation to report any security breaches or other problems, including requests for information under foreign legislation.
- Have procedures in place that allow you to act appropriately if you receive one of these reports.