THE OFFICE OF THE
Data Protection Commissioner

GPN2

Data Protection (Jersey) Law 2005

GOOD PRACTICE NOTE

Outsourcing: A Guide for Small & Medium sized Businesses

This good practice note has been published as guidance only and should be read in conjunction with the Data Protection (Jersey) Law 2005. This document gives practical advice for assisting with compliance with the Law 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 Law are important when outsourcing and provides some good practice recommendations. It applies when you use an organisation to process personal information for you, but you retain liability for the information and full control over its use.

What does the Law 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 Law.

• Outsourcing to any organisation

The Law 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 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 an appropriate and 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 require them to:

- only use and disclose the personal data in line with your instructions and in accordance with the legal requirements of the Law; and
- to take appropriate security measures.

The contract must be in place regardless of where the other organisation is based.

• Outsourcing to an organisation outside the EEA

The Law requires that where personal information is transferred to any country or territory outside the European Economic Area (EEA) 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 transcription service based in Africa, you will have to make sure that the information is adequately protected. This will apply to the method you use to send the information, as well as 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 appropriate security measures, the selection of a reputable organisation and restrictions on use 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 that country.

- You also have the option of using the model contract clauses approved by the European Commission and the UK Information Commissioner and supported by the Jersey Data Protection Commissioner for transfers to organisations acting on your behalf. These clauses can be used independently or incorporated into your main contract with the organisation. These terms can be found on the European Union website at:

http://europa.eu.int/comm/justice_home/fsj/privacy/modelcontracts/index_en.htm

These are only two of the ways of ensuring adequacy. Other ways exist depending on the particular circumstances of the transfer. Please refer to Schedule 4 of the Data Protection (Jersey) Law 2005 for further details.

Good practice recommendations

These are good practice recommendations if you want to use an organisation to process personal data on your behalf:

- 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 comprehensive, agreed and enforceable;
- Make sure the organisation has appropriate security measures in place;
- Make sure that they make appropriate checks on their staff;
- Make regular checks or audit inspections to ensure consistent standards of processing and compliance;
- Require the organisation to report any security breaches or other problems to you;
- Have procedures in place that allow you to act appropriately when you receive one of these reports.

Contacting the Commissioner:

Office of the Data Protection Commissioner
Morier House
Halkett Place
St.Helier
Jersey JE1 1DD

T. +44 (0)1534 441064
F. +44 (0)1534 441065
E. dataprotection@gov.je
W. www.dataprotection.gov.je