Data Processing Register Case Study

Example CA Firm is a medium sized accountancy practice operating within the UK. It employs a number of members of staff operating over several service lines.

The firm uses several software packages to perform tasks internal to the firm and to provide services to clients. The software is a mixture of cloud software and software hosted locally on the firms own server. The firm's servers are backed up daily using a cloud backup system.

The firm also uses e-marketing services to deliver marketing communications to clients and contacts.

The insolvency department outsource the processing of insolvent business employee claims to specialist ERA providers.

Data security policy

The firm has a Data Security Policy which sets out measures to be taken to minimise the loss of personal data. This sets out two levels of data security

Standard security	The policy sets out data security measures which the firm employs. This includes things such as password policy, server patching policy, firewalls, anti-virus protection, laptop encryption, encrypted usb flashdrives, measures to secure physical storage of files such as a clear desk policy, email attachment policy, etc. It also requires all data to be processed within the EEA or for adequate safeguards to be established where data is processed out with the EEA. (see section on Finance function below for further explanation).
Enhanced security	In addition to the standard security measures, where an enhanced level of data security is required additional measures will be put in place. This may include measures such as access being restricted to specified members of staff.

Notes on completion of data processing register

HR function
The annual fit and proper checks carried out in relation to employees and HR files have enhanced security provisions applied as these may contain information sensitive information such as criminal convictions or health issues relating to employees.

Finance function
The firm uses cloud accounting software where data farms are located in New Zealand and Canada as well as within the EEA.

New Zealand is a country where the European Commission has assessed that the country has an adequate level of protection for personal data and therefore in effect can be treated in the same way as data transferred within the EEA.

Canada is not on the list of countries which the European Commission has assessed that the country has an adequate level of protection for personal data. Data can only be transferred to non-EEA countries or countries not on the EC list of countries with adequate protection unless adequate safeguards are put in place. This can be achieved in a number of ways including using Model Contract Clauses, Binding Corporate Rules or Binding Corporate Rules for Processors (BCRs) or other contractual arrangements. Where "adequate safeguards" are established, the rights of data subjects continue to be protected even after their data has been transferred outside the EEA.

The European Commission has so far recognised the following countries as providing adequate protection:

Andorra	Argentina	Canada (commercial organisations)
Faroe Islands	Guernsey	Israel
Isle of Man	Jersey	New Zealand
Switzerland	Uruguay	USA (limited to the Privacy Shield framework)

.

IT function

The firm uses a cloud backup service where servers are located in the USA and Australia as well as within the EEA. See section on Finance function above regarding measures where data is to be transferred outwith the EEA.

Marketing function

The firm uses a CRM database and software to send bulk emails to clients and contacts.

Operational functions

The firm uses a variety of cloud and office based server software to provide its various services to clients. During the course of providing services to clients, personal data is provided to or may be accessed by a variety of governmental and regulatory agencies.