Data Processor Contract Checklist

Sharing data with third party suppliers

Wherever the Diocese intends to enter into a contract under which it will provide personal data to a third party supplier in order for the supplier to process that data on behalf of the Diocese and/or allow access by that third party to Diocesan data, it must put a written contract in place. The types of contract where this data controller – data processor relationship may arise include the outsourcing of services such as:

- Payroll provision
- HR consultancy
- Occupational health provision
- IT consultancy or the provision of IT support services
- IT management or server hosting

Please note that professional advisers such as lawyers and accountants are not deemed to be data processors under the GDPR.

The contract will set out what services are to be provided, how and at what cost, but must also set out other important provisions so that both parties understand their responsibilities and liabilities in relation to the personal data being used in the provision of those services.

The Diocese must ensure that any supplier it intends to use must provide sufficient guarantees that the requirements of the GDPR will be met and the rights of individuals whose data is being processed can be protected. Appropriate due diligence must be carried out prior to making the decision to appoint any supplier that will handle Diocesan personal data and information or certificates obtained from suppliers are documented in writing and/or retained safely.

Certain specified provisions must also be included in the contract by virtue of the GDPR. These are as follows:

Contracts must include the following compulsory details:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of data subject; and
- the obligations and rights of the controller.

Contracts must include the following compulsory terms:

- the supplier must only act on the written instructions of the Diocese (unless required by law to act without such instructions);

- the supplier must ensure that their people processing the data are subject to a duty of confidence;
- the supplier must take appropriate measures to ensure the security of processing;
- the supplier must only engage a sub-processor with the prior consent of the Diocese and a written contract;
- the supplier must assist the Diocese in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- the supplier must assist the Diocese in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- the supplier must delete or return all personal data to the Diocese as requested at the end of the contract; and
- the supplier must submit to audits and inspections, provide the Diocese with whatever information it needs to ensure that they are both meeting their obligations under the GDPR dealing with controller-processor contracts, and tell the Diocese immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

The Diocese should have a policy in place which sets out the levels and process of authorisation required for different contracts.

This checklist should be considered in conjunction with any existing internal procurement procedures.

Various additional protections should also be included within any contract with a data processor (e.g. clauses about insurance and indemnities) – please see the Data Processor Agreement for details.