**Guidance on the use of Data Processors**

**Introduction**

A third party data processor is defined under GDPR as, “a natural or legal person or organisation which processes personal data on behalf of a controller.” This essentially means any third party who processes personal data on your behalf. This could include cloud services, mailing houses, hosting companies and any other organisation whereby you share personal data as part of your business operations or as part of any projects you may be running.

Data controllers are responsible for actions taken by data processors. Therefore, you must identify all processors you use, have a clear understanding of the data you store and process with them, and understand how well each processor secures that data.

By completing an assessment of all third party processors you use, you’ll be able to gauge their awareness of GDPR. You should also be able to assess whether they have appropriate measures in place to comply with the regulations.

You should review their privacy policies and terms of use and look for GDPR statements your data processors may have prepared. This will give you clear guidance on their readiness.

A useful exercise is to map your data pathways. To understand how data is captured, what data is captured and what data is transferred between you and your data processor. This will give you a clearer understanding of your data management and where you may need to make improvements to your procedures to ensure compliance.

**Guidance from the Information Commissioner**

* Whenever a controller uses a processor it needs to have a written contract in place.
* The contract is important so that both parties understand their responsibilities and liabilities.
* The GDPR sets out what needs to be included in the contract.
* In the future, standard contract clauses may be provided by the European Commission or the ICO, and may form part of certification schemes. However at the moment no standard clauses have been drafted.
* Controllers are liable for their compliance with the GDPR and must only appoint processors who can provide ‘sufficient guarantees’ that the requirements of the GDPR will be met and the rights of data subjects protected. In the future, using a processor which adheres to an approved code of conduct or certification scheme may help controllers to satisfy this requirement – though again, no such schemes are currently available.
* Processors must only act on the documented instructions of a controller. They will however have some direct responsibilities under the GDPR and may be subject to fines or other sanctions if they don’t comply.

What needs to be included in the contract?

In brief…

Contracts must set out:

* 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 also include as a minimum the following terms, requiring the processor to:

* only act on the written instructions of the controller;
* ensure that people processing the data are subject to a duty of confidence;
* take appropriate measures to ensure the security of processing;
* only engage sub-processors with the prior consent of the controller and under a written contract;
* assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
* assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
* delete or return all personal data to the controller as requested at the end of the contract; and
* submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

**Controller and processor contracts checklist**

Our contracts 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;
* the obligations and rights of the controller.

Our contracts include the following compulsory terms:

* the processor must only act on the written instructions of the controller (unless required by law to act without such instructions);
* the processor must ensure that people processing the data are subject to a duty of confidence;
* the processor must take appropriate measures to ensure the security of processing;
* the processor must only engage a sub-processor with the prior consent of the data controller and a written contract;
* the processor must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
* the processor must assist the data controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
* the processor must delete or return all personal data to the controller as requested at the end of the contract;
* the processor must submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

As a matter of good practice, our contracts:

* state that nothing within the contract relieves the processor of its own direct responsibilities and liabilities under the GDPR.

**TEMPLATE LETTER TO SUPPLIER ACTING AS A DATA PROCESSOR ON OUR BEHALF**

To: [Insert Name and Address of Supplier]

Date:

Dear

**Re: General Data Protection Regulations**

**Contract reference [ Insert Ref.] between [Insert Name] Presbyterian Church and [Insert Supplier Name] refers**

New data protection legislation (“General Data Protection Regulation”) is due to come into force during May 2018, which aims to protect the privacy of all EU citizens and prevent data breaches. It will apply to any public or private organisation processing personal data.

Established key principles of data privacy will remain relevant in the new data protection legislation but there are also a number of changes that will affect commercial arrangements, both new and existing, with our suppliers. The General Data Protection Regulation specifies that any processing of personal data, by a processor, should be governed by a contract with certain provisions.

Our existing contract, [contract reference] with you involves processing of personal data and, as this will be in place after 25 May 2018, may require updating to bring it into line with the Regulation. This will involve updating contract terms to ensure specifications in service delivery reflect your role and responsibilities as processor of personal data for which we are controller.

We attach at Appendix 1 our proposed amendment to our contract with you, for your review and consideration. Please confirm your acceptance of this amendment by signing and returning a copy of Appendix 1. If you have any issues or concerns with this, or wish to propose alternative terms to comply with the new Regulation, please contact [Insert Contact Details] to discuss the way forward.

As you will be aware, as a controller, we will not accept liability clauses where you are indemnified against fines under GDPR as the processor. A legal penalty regime has been extended directly to processors to ensure better performance and enhanced protection for personal data. That means indemnifying processors for any GDPR fines or Court claims would undermine these principles.

We look forward to receiving your confirmation of agreement to the attached or alternative proposals to vary our existing contract to comply with the new Regulation.

Yours sincerely

................................................................

[NAME OF SENDER – printed under signature]

For and on behalf of [Insert name of Presbytery or Congregation]

**Appendix 1**

* 1. Data Protection

The Contractor acknowledges that in performing the Services under [Insert Contract Identifier] **(the Contractor**) shall process personal data within the meaning of [Data Protection Law] on behalf of [Insert Church Name] Presbyterian Church (**the Church**). The Contractor agrees that:

* + 1. the Contractor processes such personal data and for such purposes as are set out in Annex 1 (*Data Protection)* or otherwise agreed in writing between the parties, on behalf of the Church in the context of providing the Services under this contract, for the duration of the term of this contract. The obligations and rights of the Church shall be as set out in this [amendment to the contract];
    2. the Contractor shall only process such personal data in accordance with the documented instructions of the Church, including with regard to transfers of such personal data to a third country and solely as strictly necessary for the performance of its obligations under this contract;
    3. the Contractor shall ensure that the persons authorised by the Contractor to process such personal data are bound by appropriate confidentiality obligations;
    4. the Contractor shall implement such technical and organisational security measures as are required to comply with the data security obligations under Data Protection Law;
    5. the Contractor shall not engage any sub-processor without the prior general written authorisation of the Church and where the Church has provided a general authorisation to the appointment of sub-processors, the Contractor shall inform the Church if it intends to replace a sub-processor or engage other sub-processors, and provide the Church with an opportunity to object to such changes;
    6. where any Sub-Contractor of the Contractor will be processing such personal data on behalf of the Church, the Contractor shall ensure that a written contract exists between the Contractor and the Sub-Contractor containing clauses equivalent to those imposed on the Contractor in this clause 1.1 (*Data Protection*). In the event that any sub-processor fails to meet its data protection obligations the Contractor shall remain fully liable to the Church for the performance of the sub-processor’s obligations;
    7. the Contractor shall assist the Church by implementing appropriate technical and organisational measures to enable the Church to comply with requests from data subjects to exercise their rights in respect of such personal data under Data Protection Law;
    8. the Contractor shall assist the Church in ensuring compliance with its obligations in respect of the security of such personal data, data protection impact assessments and prior consultation requirements under Data Protection Law;
    9. when the Contractor ceases to provide services relating to data processing the Contractor shall:
       1. at the choice of the Church, delete or return all such personal data to the Church; and
       2. delete all existing copies of such personal data unless EU law, UK law or the laws of an EU Member State require storage of the personal data;
    10. the Contractor shall:
        1. make available to the Church all information necessary to demonstrate compliance with the obligations laid down in this clause 1.1 (*Data Protection*); and
        2. allow for and assist with audits, including inspections, conducted by the Church or another auditor mandated by the Church, in order to ensure compliance with the obligations laid down in this clause 1.1 (*Data Protection*), provided that the Church shall be entitled at its discretion, to accept adherence by the Contractor to an approved code of conduct or an approved certification mechanism to aid demonstration by the Contractor that it is compliant with the provisions of this clause 1.1 (*Data Protection*);
    11. the Contractor shall inform the Church immediately if, in its opinion, it receives an instruction from the Church which infringes Data Protection Law;
    12. the Contractor shall notify the Church immediately after becoming aware of any personal data breach in relation to such personal data and provide the Church with such reasonable co-operation and assistance as may be required to mitigate against the effects of, and comply with any notification obligations which may apply in respect of, any such personal data breach; and
    13. no such personal data shall be transferred outside of the European Economic Area by the Contractor or its Sub-Contractors or any agents without the prior approval of the Church which approval may be subject to terms and conditions (including that the data importer enters into a contract incorporating standard contractual clauses in the form approved by the European Commission and, where relevant, complies with the provisions regarding sub-processors contained in such standard contractual clauses in respect of any sub-processors). The Contractor shall comply with the requirements of Data Protection Law in respect of transfers of such personal data outside of the European Economic Area, to the extent that the Church consents to any such transfer.

[Signature] \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[Print Name] \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[On behalf of] \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_