ACCOUNTING TECHNICIANS IRELAND

PROCEDURE FOR ENGAGING DATA PROCESSORS

GENERAL DATA PROTECTION REGULATIONS (GDPR)

Document Control

Owner: Data Protection Officer

Distribution List: Relevant individuals who would negotiate the contract with third party Data Processors on behalf of Accounting Technicians Ireland (ATI)

VERSION NUMBER	DATE	DETAILS OF REVISIONS
1.0	July 2017	Document created

1.0 Procedure for Engaging Data Processors

ATI as the Data Controller will on occasions need to engage the services of a sub-contractor or agent to process personal data on its behalf. Such an agent is termed a 'Data Processor' under the General Data Protection Regulations (GDPR). GDPR place responsibility for the duty of care owed to personal data on the Data Controller and therefore this cannot be passed over to the Data Processor.

In accordance with the GDPR, ATI will only engage with a data processor on the basis of a written contract (or a contract in equivalent form), who will guarantee compliance with this Regulation and ensure the protection of the rights of the data subject. Informal and ad-hoc arrangements will not be acceptable, where personal data is involved. An example to demonstrate sufficient guarantees could be adherence to either an approved certification mechanism or an approved code of conduct.

The Data Protection Officer will maintain a list of all third-party processers, type of contract ATI have with each one and the processing location. Contract types can vary, see below:

1.1 Contracts with 3rd Parties within the European Economic Area (EEA)

All contracts will vary depending on the particular circumstances arising, but as a general rule ATI will consider the inclusion of the following key points when drafting or reviewing a contract:

- ATI relationship with any Data Processor will be governed by a contract (or a contract in equivalent form) which will be binding on the processor with regard to the controller and sets out the following:
    - Subject matter and duration of the processing
    - Nature and purpose of the processing
    - Type of personal data
    - Categories of data subjects
    - Obligations and rights of the controller
- The contract or equivalent shall stipulate, in particular per Article 28, that the processor:
    - Processes the personal data only on documented instructions from ATI, including transfers of the personal data to a country outside the EEA (third country) or an international organisation, unless required to do so by

the Union or Member State Law to which the processor is subject to. The Processor must inform the Controller of that legal requirement before processing, unless that law prohibits this on the grounds of public interest;

- Ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

- Ensures the security of the personal data that it processes;

- The processor cannot engage another processor without prior specific or general written authorisation from ATI. The processor cannot replace a processor without informing the company, thereby giving ATI the opportunity to object to such changes.

- Taking into account the nature of the processing, assist ATI by appropriate technical and organisational measures, insofar as this is possible, in order that ATI can fulfil its obligation to respond to Data Subject's Rights requests.

- Assist ATI in ensuring compliance with the following obligations, taking into account the nature of the processing and the information available to the processor:

    - Security of processing – processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

    - Notification of a personal data breach to the supervisory authorities – the processor should notify Data Protection Officer, both verbally and in writing to the designated email address XXX without undue delay after becoming aware of a data breach.

- Data protection impact assessment – if the processor begins using new technologies and the nature, scope, context and purpose(s) of the processing is likely to result in a high risk to the rights and freedoms of a natural person, the processor shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data

- Prior consultation from the supervisory authority regarding the data protection impact assessment – If the data protection impact assessment highlights a high risk in the absence of measures taken by the processor to mitigate the risk.

- At the choice of ATI, the processor deletes or returns all the personal data to the company after the end of the provision of services relating to processing and deletes existing copies unless Union or Member state law requires retention of the personal data.

- Makes available to ATI, all information necessary to demonstrate compliance with the obligations laid down under the GDPR and allow for and contribute to audits, including inspections, conducted by the company or an auditor mandated by the company. The processor can demonstrate compliance to ATI by either providing an approved certification or code of conduct.

1.2 Contracts with 3rd Parties outside the European Economic Area (EEA)

ATI on occasions may need to transfer personal data to processors/recipients outside the EEA, for example cloud-based services. ATI will adhere to the GDPR and only transfer data for processing to a Data Processor if:

- the jurisdiction in which the recipient is located is deemed to provide an adequate level of data protection;

Or

- ATI has put in place appropriate safeguards;

In such situations ATI will ensure that the processor/recipient has an adequate level of data protection safeguards and on condition that enforceable data subject rights and effective legal remedies for data subjects are available and which provide ATI with a lawful basis on which to transfer data. ATI will adhere to the cross-border rules as outlined in the GDPR by ensuring that:

- The country is on the EU Commission "approved list", which can be viewed on the EU Commission website www.ec.europa.eu

- If the country is not on the approved list, ATI will use a Model Contract, except if it is the USA. A 'model contract' is a general type of contract that includes specific provisions, "model clauses" dealing with data protection, and that has been approved by the EU Commission. ATI will use the template provided on the EU Commission website www.ec.europa.eu

- If the country is not on the approved list, ATI have the option to rely on approved Codes of Conduct (i.e. codes of conducts provide a means for certain industry sectors, to create context-specific rules regarding the processing of personal data in their particular industry sector in compliance with GDPR) together with binding and enforceable commitments to provide appropriate safeguards. Transfers made on this basis do not require approval from the ODPC

- If the country is not on the approved list, ATI can make a cross-border data transfer on the basis of the recipient having an approved certification. The certification provides ATI with a formally recognised confirmation of compliance with GDPR.

- If the country is not on the approved list, ATI are aware that they can draft Irish-specific contracts. These are contractual clauses, which need not conform exactly to the EU Commission's 'model clauses', however these clauses still need to provide adequate data protection safeguards and need to be approved by the ODPC. ATI has decided that these would not be considered because the model clauses in the model contracts are a well-known proven concept.

- If the data is being processed in the USA, ATI will ensure that the Data Processor is a part of the
    - EU-USA Privacy Shield - which is a framework that protests the fundamental rights of anyone in the EU whose personal data is transferred to the United States i.e. server based in the US, as well

as bringing legal clarity for businesses relying on transatlantic data transfers. As this is a self-certifying, voluntary scheme therefore ATI will adopt the motto 'Trust by verify' i.e. ATI will to the best of its ability verify that the Data Processor has adequate protection in place to protect the company's data. This will be ATI's preference, but if a business decision requires a processor to be used which is not a member of the Privacy Shield, then ATI will adopt a Model Contract.

1.3 Service Agreements/Terms of Use from 3rd Parties Service Providers

ATI engages with large service providers which only provide standard terms of use and service agreements. In this case ATI will research to see if the same level of service can be provided by a processor within the EEA, however if this is not feasible, and it is a business decision to proceed then the company will ensure that:

- The service is clearly stated and processing of personal data is limited to the provision of this service.
- Appropriate safeguards regarding data subject rights.
- Adequate security measures will be applied to safeguard the personal data from unauthorised access or disclosure.
- It clearly states what occurs to the personal data on termination or ending of the contract.
- That there are standard data protection clauses adopted within the agreement.

1.4 Contracts with 3rd Party Payment Service Providers

In addition to following the appropriate procedure outlined above in relation to the chosen payment service provider(s), ATI will also ensure that there is a high level of security when dealing with such a processor i.e. it will not engage in a contract unless the service provider is PCI compliant.

1.5 Clear segregation of responsibilities within a contract between ATI and Data Processor is paramount

GDPR states that any person who has suffered "material or non-material damage" as a result of a breach/infringement of this Regulation has the right to receive compensation from either the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress and hurt feelings even where they are not able to prove financial loss.

The responsibility lies with ATI, however a processor will be liable for the damage caused by processing only where they has not complied with obligations relating to processors as directed by this Regulation (as outlined above) or where they have acted outside or contrary to lawful instructions from ATI

Therefore, it is paramount that a clear segregation of responsibilities is outlined in any contract between ATI and a Data Processor to ensure that if such a claim is levied against ATI, it will be easily identified as to who is liable to pay the compensation, if any.