This document is part of a larger suite of guidance resources for anyone who is using third parties to perform certain tasks with people's data, please refer to www.odpa.gg/information-hub/guidance/engaging-processors for a general overview of this area, together with several detailed guidance resources.

Guidance 2: Processor assessments

This guidance is for anyone who wants to know more about how to assess a processor's suitability.

Controller and processor obligations under the Law

Both controllers and processors are obliged under the Law to put in place appropriate technological and organisational measures to ensure the security of any personal data they process. These technological and organisational measures may include:

- encryption and pseudonymisation;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore access to personal data in the event of an incident; and
- processes for regularly testing and assessing the effectiveness of the measures.

Further, The Law requires that a legally binding contract is put in place between you, as controllers, and your processors to formalise their respective obligations under the Law. Contract considerations are outlined in companion guidance entitled 'contracts between controllers and processors'[1].

The level of technological and organisational measures should also be commensurate to the nature of the data and processing itself, including the degree of sensitivity of data (e.g. special category data) and the context of the processing (e.g. for a health clinic versus a tennis club). For further guidance on these please see 'Data Protection by Design and Default'[2].

Please refer to the Templates[3] guidance area for a set of Controller and Processor questionnaires which will help you consider your compliance with this area of the Law.

What responsibilities does a controller have when using a processor?

When you appoint a processor to carry out work on your behalf you are, in effect, trusting this party with the personal data entrusted to you. This appointment should be a considered decision, you should evaluate the suitability of the processor and carry out an assessment[4] of the technical and organisational measures the processor has in place to keep personal data safe.

This formal assessment should take into account the nature of the processing and the risks to the data subjects and you should ensure that the processor has provided "sufficient guarantees" (in particular in terms of its expert knowledge, resources and reliability) that it has implemented appropriate technical and organisational measures to ensure that their processing:

- meets the requirements of this Law; and
- safeguards data subject rights

In practice, your consideration could include:

[1] See: www.odpa.gg/information-hub/guidance/engaging-processors
[2] See: www.odpa.gg/information-hub/guidance/dpia/data-protection-by-design-and-default/
[3] See: www.odpa.gg/information-hub/guidance/templates/
[4] See Appendix 1 at the end of this document for a non-exhaustive list of questions you can pose to your processors in order to assess their suitability.

- the extent to which they comply with industry standards, if these apply in the context of the processing
- whether they have sufficient technical expertise to assist the controller in carrying out obligations under the Law (technical measures, breach notifications and DPIAs)
- providing the controller with relevant documentation, e.g., their privacy policy, record management policy and information security policy
- adherence to an approved code of conduct or a certification scheme (where relevant)
- whether the processor is engaging a secondary processor[5] and if so, if they are complying with the Law in this regard
- whether there is a risk that the processor would use any data shared for secondary purposes, neither prescribed nor authorised by the controller
- whether the processor is storing, processing or transferring any personal data outside an authorised jurisdiction, and, if so, how they are complying with the Law.

This is not an exhaustive list, and ultimately it is for the controller to satisfy itself that the processor provides sufficient guarantees in the context of the processing. Whether the guarantees are sufficient will depend on both the circumstances of the processing and the risk posed to the significant interests of individuals. Use Appendix 1 below to assist you.

Ongoing responsibilities of controllers regarding processors

You should ensure a processor's compliance on an ongoing basis, in order for you to satisfy the Law's accountability principle and demonstrate due diligence. In particular, the Law explicitly requires the processor to allow for and contribute to audits and inspections, carried out either by the controller or a third party appointed by the controller. The methods used to monitor compliance and the frequency of monitoring will depend on the circumstances of the processing.

[5] See: 'Controller, Joint Controller, Processor or Secondary Processor' guidance at: www.odpa.gg/information-hub/guidance/engaging-processors

Appendix 1 – Processor assessment consideration

This document has been prepared for completion by the processor. Their answers to these questions should assist you as the controller in assessing the processors you work with.

DATA COLLECTION

Question 1: What personal data is processed? (e.g. name, address, telephone number etc.)

Question 2: Why is this personal data processed? For what purpose/purposes is it used?

Question 3: Within the Law, the term "special category data" replaces the previous legal term "sensitive personal data". It also encompasses more data types than the previous definition. (See Note 2 in the Processors' Self-Assessment Notes[6] for more information on "sensitive personal data" and "special category data") With the expanded definition in mind, is any special category data held or processed (e.g. medical/health data, ethnic origin etc.)? If so, for what purpose?

GOVERNANCE

Question 4 Do you have a Data Protection Officer?

Question 5 If so, to whom does the Data Protection Officer report?

Question 6 What responsibilities does the Data Protection Officer have?

Question 7 If you do not currently have a Data Protection Officer, are you planning to appoint someone?

Question 8 Are written agreements in place between your organisation and the controller that outline how personal data should be processed?

Question 9 If yes, how often are these reviewed and updated?

STORAGE AND ARCHIVING

Question 10 How does your organisation store personal data on behalf of a controller? (e.g. on computer or manual files or both and/or on personal devices?) Set out details of all databases/filing systems containing personal data.

Question 11 If personal data is stored on computer is this located within the organisation or elsewhere? If elsewhere, identify the third party storing the data, detailing where and how the data is stored.

Question 12 If personal data is stored manually is this within the organisation or elsewhere? If elsewhere, identify the third party (sub-processor) storing the data, detailing where and how the data is stored.

Question 13 If your organisation processes special category data on behalf of a controller, is such data stored separately from any other personal data or subject to any specific marking, security or handling rules/restrictions?

[6] See: https://www.odpa.gg/information-hub/guidance/templates

Question 14 In what format or in what medium is the archived data stored?

Question 15 Where is the archived data stored? If it is stored on third party premises, identify that third party and where and how it is stored?

SECURITY

Question 16 Describe the security procedures in place in your organisation to keep all personal data processed on behalf of a controller secure. Describe the physical, administrative and technological procedures used and any specific requirements each controller may have.

Question 17 Who has access to personal data within the organisation/outside the organisation?

Question 18 Who controls and authorises such access?

Question 19 Do you have policies and procedures in place for detecting and dealing with breaches? If so, what are they?

Question 20 How do you check that there has been no internal unauthorised access to personal data? What data audit facilities/mechanisms are in place?

Question 21 What are your procedure for reporting breaches to the controller?

DESTRUCTION OF DATA AND TERMINATION OF CONTRACT

Question 22 Under the contract with the controller, are you responsible for the destruction of the personal data?

Question 23 How is personal data destroyed?

Question 24 Who authorises destruction? Who carries out destruction? What agreements are in place with contractors who provide shredding etc. facilities/services?

Question 25 Are there clear instructions in the contract detailing what happens to the personal data at the end of the contract period?

USING SECONDARY PROCESSORS

Question 26 Are any of your personal data processing activities carried out by third parties (secondary processors)? List them and describe the processes and location of the provider and the data.

Question 27 Who authorises these processing activities?

Question 28 Are written agreements in place covering these arrangements?

Question 29 Outline the security measures under which each sub-processor must operate

Question 30 Do the secondary processors used by your organisation use any other organisation to perform that service on their behalf? If so, list the organisation and detail the written arrangements in place with regards to the service these sub-contractors offer.

This document is part of a larger suite of guidance resources for anyone who is using third parties to perform certain tasks with people's data, please refer to www.odpa.gg/information-hub/guidance/engaging-processors for a general overview of this area, together with several detailed guidance resources.

SECONDARY USES OF DATA BY THE PROCESSOR

Question 31 Does the processor's business operations include uses of data for its own commercial purposes (e.g. analytical processing and the selling of market trend data)?

Question 32 If there is an agreement with the processor for secondary uses of data does it comply with data protection requirements (e.g. transparency, consent, etc.)

TRANSFERS OF PERSONAL DATA

Question 33 Do you transfer data cross-departmentally and/or to third parties outside the organisation?

Question 34 How is data transferred? (e.g., Encrypted email? Secure fax?)

Question 35 In what countries are those people to whom you disclose the information (whether inside the organisation or external) located?

Question 36 Where personal data is transferred outside the EEA, what measures are used to ensure compliance with the Law (Part X)?

TRAINING

Question 37 Do the employees in your organisation receive training on data protection and other relevant law? If so, describe the nature of the training given, when it is given and identify who is responsible for carrying out the training.

Question 38 Are refresher courses held? If so, describe the nature of the training given, when it is given, identify who is responsible for carrying out the training and who is directed to attend.

Question 39 Have the following attended a data protection awareness session?
a. The Board
b. Senior management
c. Security/IT team
d. All other staff