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 3: Contracts between controllers and processors

This guidance is for anyone who wants to understand the Law's requirements for contracts between parties who are working together on activities that involve personal data.

Why are contracts between controllers and processors important?

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. Aside from the legal requirements, this makes practical and commercial sense by:

- ensuring all parties comply with the Law;
- protecting the personal data of customers, staff and others; and
- ensuring all parties are clear about their role regarding the personal data that is being processed and are able to demonstrate this.

What information is required to be included in the controller / processor contracts?

The Law requires the following information to be included in the contract between you and a processor.

(a) the subject matter of the processing
(b) the duration of the processing
(c) the nature, scope, context and purpose of the processing
(d) the category of personal data to be processed
(e) the categories of data subjects
(f) the duties and rights of the controller and
(g) the duties imposed on the processor by sections 35 and 36.

You can learn more about each of these areas in Appendix 1 below.

Who should be party to the contract?

Both you and the processor must be party to the contract. In any secondary processing arrangements, the relevant parties to the contract will be the processor and secondary processor.

For organisations with no separate legal personality (e.g., unincorporated partnerships or unincorporated associations), you should review the document which sets up and governs the management of that organisation. This document should set out which individual(s) manage the organisation on behalf of its members and are likely to act as the controller or joint controllers, and how contracts may be entered into on behalf of the organisation.

Can standard contract clauses (SCCs) be used?

The EU has issued "Standard Contractual Clauses for Controllers and Processors (EU 2021/3071)" that include contracts between controllers and processors.

These clauses may provide a simple way for you to ensure that contracts between you and your processors comply with the Law.

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.

Appendix 1: controller/processor contract requirements in plain English

The Law requires the following to be included in the contract:

The subject matter of the processing

This section should describe the service the processor is providing to you that involves the processing of personal data.

Example (Outsourced HR and payroll)

"Providing outsourced HR and payroll services"

The duration of the processing

This section should outline how long the personal data will be processed. This is usually the duration of the service provided, plus any retention period requested by you.

Examples (General)

"Duration of the contract"

"In accordance with Clause 21 of the master service agreement"

"Until instructed to delete by the Controller"

The nature, scope, context, and purpose of the processing

This section should explain the processing being conducted including**:**

- *Nature:* **Type** of processing occurring
- *Scope:* **How much** personal data will be processed
- *Context:* **Why** the processing is necessary
- *Purpose*: **Why** the processing is occurring

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.

Example (outsourced IT services)

IT Genius has been appointed by ABC Company to provide outsourced IT solutions (i.e. helpdesk, IT management and cyber security support) in accordance with a 'Master Service Agreement', dated 23 June 2020.

These services will include IT Genius being provided with access to all data (including all personal data) held within the servers of ABC Company. The data will only be accessed when required and requested by ABC Company.

IT Genius require access to this data (and personal data) to allow them to assist with all IT issues raised by the teams and to ensure that the system remain secure.

ABC Company has no inhouse IT team therefore this appointment will allow for the smooth operations of the business and the prompt resolution of issues.

The category of personal data to be processed

This section should outline the types of personal data that would be processed by the processor.

Example (outsourced delivery services)

The processor will be provided with access to the following personal data:

- Name of the customers
- Address of the customers
- Phone number of the customers
- Delivery preferences of the customers

The categories of data subjects

This section should outline the types of individuals personal data will be processed about by the processor.

Example (outsources HR and payroll)

The categories of data subject include:

- Current employees
- Past employees
- Prospective employees
- Directors
- Contractors and work experience students

The duties and rights of the controller

Duties of the controller when acting as a joint controller

Where two or more controllers jointly determine the purpose and means of processing the same personal data, they are joint controllers.

Joint controllers **must** clearly agree on their respective responsibilities to comply with the Law. Specifically:

1. They must agree on their roles and duties.
2. This agreement should detail their roles, relationships, and responsibilities, and it may include a contact point for data subjects.
3. They must inform data subjects about these roles and responsibilities.
4. Data subjects can exercise their rights with any joint controller, and each controller is fully responsible for compliance with the law.
5. These requirements do not apply if the law already clearly defines the responsibilities of the joint controllers.

Duties of the controller in relation to processors

A processor is any party that is given the task of processing personal data by and on behalf of a controller.

A controller **must** not allow a processor to process personal data unless the following two conditions are met:

1. The processor must guarantee the controller that it will implement reasonable technical and organisational measures to comply with the Law and protect the rights of data subjects.
2. There must be a legally binding written agreement between the controller and the processor that specifies:

- The **details** of the processing.
- The **duration, nature, scope, context,** and **purpose** of the processing.
- The **types** of personal data and **categories** of data subjects involved.
- The **responsibilities** and **rights** of the controller.
- The **duties** of the processor as required by sections 35 and 36 of the Law.

Additionally, whether the processor follows an approved code or mechanism can influence the assessment of these guarantees.

Ongoing duties of the controller

Controllers are required to ensure that they comply with the following 6 points in all circumstances:

1. **Record Keeping:** Controllers and processors must keep required records for specified periods.

2. **Inspection Compliance:** Controllers must produce records for inspection or provide them upon request by the Data Protection Authority.

3. **Information Returns:** Controllers must provide information returns as required by the Data Protection Authority.

4. **Cooperation with Authority:** Controllers and processors must cooperate with the Data Protection Authority in its functions, including complying with information notices and facilitating data protection audits.

5. **Access and Compliance:** Where required, controllers must allow officers of the Data Protection Authority entry to premises, access to information and must comply with enforcement orders if issued.

6. **Registration:** If an entity works with data about or related to identified (or identifiable) living people, it is legally obliged to maintain an annual registration.

The duties imposed on the processor by sections 35 and 36

Please refer to Appendix 2 below for more information on this aspect of the Law.

Appendix 2: The duties imposed on processors by sections 35 and 36

Section 35 and 36 of the Law sets out the following specific obligations for processors:

1. Processing only on the documented instructions of the controller
2. Duty of confidence
3. End-of-contract provisions
4. Reasonable technical and organisational measures
5. Assisting the controller with compliance with the Law in regard to Data Protection Impact Assessments (DPIAs) and security of personal data
6. Audits and inspections
7. Using sub-processors

Each of the above areas are explored further below. These areas are the minimum requirements, but you may agree with the processor to supplement them with your own terms.

1. *Processing only on the documented instructions of the controller*

The Law requires that the processor must only process personal data based on written instructions from you (including with regard to transfers of personal data to an unauthorised jurisdiction) unless it is required to do otherwise by law.

Where a processor is required by law to process personal data contrary to the instructions of the controller it must inform you, unless it is prohibited by an enactment, before doing so.

In practice:

- the instruction can be documented using any written form, including email. A record should be retained of the instruction.

- the contract term should make it clear that you, rather than the processor, has overall control of what happens to the personal data.

If a processor acts outside of your instructions in such a way that it decides the purpose and means of processing, including to comply with a statutory obligation, then it will be considered to be a controller in respect of that processing.

2. Duty of confidence

The Law requires the processor to legally bind any party it allows to process the personal data to a duty of confidentiality.

In practice:

The processor should ensure that the duty of confidentiality covers the processor's employees as well as any temporary workers and agency workers who may have access to the personal data.

3. End-of-contract provisions

The Law requires that at the end of the provision of services provided, the processor either:

- deletes all personal data; or
- returns all personal data to you, and deletes existing copies

This reflects the fact that it is ultimately the controller that decides what should happen to the personal data being processed, once processing is complete.

The only exception to this is where personal data needs to be retained to comply with a legal duty.

In practice:

- Deletion of personal data should be done in a secure manner, in accordance with the Law.
- The contract should include terms to ensure the continuing protection of personal data after the contract ends.
- It may not be possible for data in backups or archives to be deleted immediately on termination of a contract. Provided appropriate safeguards are in place, such as the data being put immediately beyond use, it may be acceptable that the data is not deleted immediately if the retention period is appropriate and the data is subsequently deleted as soon as possible, e.g., on the processor's next deletion/destruction cycle.

4. Reasonable technical and organisational measures

The Law requires that the processor put in place reasonable technical and organisational measures to assist you in exercising or performing your duties in regard to data subject rights.

In practice:

- The processor will need to help you respond to data subject requests by searching their systems and files to identify any personal data processed. This personal data would then need to be either provided, rectified, erased or processing limited depending on the request(s) of the data subject.

5. Assisting the controller with compliance with the Law in regard to Data Protection Impact Assessments (DPIAs) and security of personal data

Under the Law the processor must, while considering the nature of the processing and the information available, assist the controller in meeting its obligations to:

- keep personal data secure
- notify personal data breaches to the controller as soon as practicable
- assist with the completion of DPIAs when required

In practice:

Contracts should be as clear as possible about how the processor will help you meet your obligations. Read our guidance on 'Processor assessments'[1] to assess the security of processors technological and organisational controls outline more areas to consider in this regard.

6. Audits and inspections

Under the Law processors must:

[1] This guidance is available at: www.odpa.gg/information-hub/guidance/engaging-processors

- provide you with any information needed to demonstrate compliance with sections 34-36 (Duties of controllers and processors in relation to each other and processing activities) of the Law.
- facilitate any lawful audits or inspections, including any inspections conducted by the controller, an auditor authorised by the controller or as required by or under the Law

In practice:

- The processor could demonstrate compliance by giving you the necessary information or by submitting to an audit or inspection.

- The Law does not require a processor to keep records of the processing it carries out for you. However requirements for processors to maintain records of their processing activities are set out in the Law.

7. Using secondary processors

A processor is not permitted to engage another processor (secondary processor) to process personal data unless:

- You have specifically authorised the secondary processor to process the personal data; or

- You have generally authorised the engagement of secondary processors and the processor has notified you of the proposed engagement, and given you an opportunity to object to the engagement

Where a processor does appoint a secondary processor, they must ensure that the same legal and contractual conditions are imposed on the secondary processor as are required by the Law to be imposed on the processor. This should include the secondary processor providing sufficient guarantees to implement appropriate technical and organisational measures in respect of processing to meet the requirement of the Law.

In practice:

- the wording of these obligations does not need to exactly mirror those set out in the contract between the controller and the processor, but should offer an equivalent level of protection for the personal data
- the processor is liable to you for a secondary processor's compliance with its data protection obligations.