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 1: Controller, Joint Controller, Processor or Secondary Processor?

This guidance is for anyone who wants to understand the different roles played when you are working with others on an activity that involves information about people (personal data).

Roles, responsibilities, and relationships

Before you read the guidance below it is important to understand that **any entity who is working with personal data** is likely to be a controller it its own right when it is working with personal data to achieve its own goals.

However, you need to understand the roles of processors, joint controllers etc. when you start working with other parties to do something with personal data. When this happens, the relationship between yourself and the other parties and the relative roles you play in the specific activity you are working together on need to be defined.

A key consideration is determining which party is deciding on the purposes and manner of the specific processing, and who is working under instruction.

What is a controller?

Controllers are the main decision-makers – they exercise overall control over the purposes and means of the processing of personal data. Controllers are any party that is **responsible for the decisions made** about **why** and **how** personal data is collected and stored about staff, customers, suppliers, or any other individuals.

Example
ABC Limited runs a small restaurant in St Peter Port. As part of its employment process, it decides to collect name, address, detail of past employment, permits and health and safety certificates for all employees. These items of personal data are retained in the employee's HR files until 6 years after the last shift worked.

Note: **Employees** of the controller are not usually controllers in their own right. As long as they are acting within the scope of their duties as an employee, they are acting as an agent of the controller itself. They are **part of the controller**, not a separate party contracted to process data.

What is a processor?

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

Processors do **not** determine the nature or the means of the processing, they just do what the controller tells them to do. In doing so, they serve the controller's interests rather than their own.

Although a processor may make its own day-to-day operational decisions, the Law says it should only process personal data in line with a controller's instructions, unless it is required to do otherwise by law.

If a processor acts without the controller's instructions in such a way that it determines the purpose and means of processing, including to comply with a statutory obligation, it will become a controller in respect of that processing and will have the same liability as a controller.

A processor can be a company or other legal entity (such as an incorporated partnership, incorporated association or public authority), or an individual, for example, a consultant.

Example
A gym engages a local printing company to produce invitations to a special event the gym is hosting. The gym gives the printing company the names and addresses of its members from its member database, which the printer uses to address the invitations and envelopes. The gym then sends out the invitations.

The gym is the controller of the personal data processed in connection with the invitations. The gym determines the purposes for which the personal data is being processed (to send individually addressed invitations to the event) and the means of the processing (mail merging the data subjects' name and address details). The printing company is a processor processing the personal data only on the gym's instructions.

Note: **Employees** of the processor are not processors. As long as they are acting within the scope of their duties as an employee, they are acting as an agent of the processor itself. They are **part of the processor**, not a separate party contracted to process data on the controller's behalf.

What is a secondary processor?

A processor might wish to use the services of another processor to assist them. Where a processor outsources to another processor, this party is called a secondary processor.

What are joint controllers?

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

Joint controllers must arrange between themselves who will take primary responsibility for complying with Law, and in particular transparency obligations and individuals' rights. They should make this information available to individuals.

However, all joint controllers remain responsible for compliance with the controller obligations under the Law. Both the ODPA and individuals may take action against any controller regarding a breach of those obligations.

How to determine whether you are a controller, joint controller, processor or secondary processor?

Controller and joint controller

To determine whether you are a controller, joint controller, processor or secondary processor, you will need to consider your role and responsibilities in relation to your data processing activities.

Again, it is important to remember that an organisation is not, by its nature, either a controller or a processor. Instead, you need to consider the personal data and the processing activity that is taking place and consider **who** is determining the purposes and the manner of that specific processing. This could including considering which organisation decides:

- to collect personal data in the first place
- the lawful basis for doing so
- what types of personal data to collect
- the purpose or purposes the data are to be used for
- which individuals to collect data about
- whether to disclose the data, and if so, to whom
- what to tell individuals about the processing
- how to respond to requests made in line with individuals' rights; and
- how long to retain the data or whether to make non-routine amendments to the data.

These are decisions that determine the purposes and means of the processing. Therefore, if you make any of these decisions, it is likely that you are a controller.

In summary if you exercise overall control of the purpose and means of the processing of personal data – i.e., you decide what data to process and why – you are a controller.

If you work with another controller to jointly determine the data you collect and process, you may be a joint controller.

Processor and secondary processor

If you only act on a client's instructions, you are likely to be a processor – even if you make some technical decisions about how you process the personal data. In certain circumstances, and where allowed for in the contract, a processor may have the freedom to use its technical knowledge to decide how to carry out certain activities on the controller's behalf. This could include deciding:

- what IT systems or other methods to use to collect personal data
- how to store personal data
- the details of the security measures to protect personal data

- how it will transfer personal data from one organisation to another
- how it will retrieve personal data about certain individuals
- how it will ensure it adheres to a retention schedule and
- how it will delete or dispose of the data.

However, if you are a processor you cannot take any of the overarching decisions, such as what types of personal data to collect or what the personal data will be used for. Such decisions must only be taken by the controller.

If you have been engaged by another processor to assist them carry out the work assigned to them by a controller, you are likely to be a secondary processor.

Why is it important to distinguish between controllers and processors?

Your obligations will depend on whether you are a controller or processor. Therefore, it is important that you carefully consider your role and responsibilities in respect of your data processing activities, so you understand:

- your obligations and how to meet them
- your responsibilities to individuals and supervisory authorities (including the ODPA) and the penalties associated with non-compliance, such as fines and other enforcement powers and
- how you can work with other organisations to ensure you process personal data responsibly and respect individuals' rights.

If you are a controller, you will have more obligations under the Law as you will decide what personal data is collected and why, and exercise ultimate control over the data.

If you are a processor, you will have fewer obligations but must be careful to only process personal data in line with the relevant controller's instructions.

Can you be both a controller and a processor of personal data?

Yes. If you are a processor that provides services to other controllers, you are very likely to be a controller for some personal data and a processor for other personal data.

- For example, you will have your own employees so you will be a controller regarding your employees' personal data. However, you cannot be both a controller and a processor for the same processing activity.

In some cases, you could be a controller and a processor of the same personal data – but only if you are processing it for different purposes.

- For example, you may be processing some personal data as a processor for the controller's purposes and only on its instruction, but also process that same personal data for your own separate purposes.

In particular, if you are a processor, you should remember that as soon as you process personal data outside your controller's instructions, you will be acting as a controller in your own right for that element of your processing.

If you are acting as both a controller and processor, you must ensure your systems and procedures distinguish between the personal data you are processing in your capacity as controller and what you process as a processor on another controller's behalf. If some of the data is the same, your systems should be able to distinguish between these two capacities and allow you to apply different processes and measures to each. If you cannot do this, you are likely to be considered a joint controller rather than a processor for the data you process on your client's behalf.

Appendix 1 - Am I a controller?

You are likely to be a controller if you answer 'yes' to one or more of these questions in relation to a given set of processing.

☐ We decided to collect or process the personal data.

☐ We decided what the purpose or outcome of the processing was to be.

☐ We decided what personal data should be collected.

☐ We decided which individuals to collect personal data about.

☐ We obtain a commercial gain or other benefit from the processing, except for any payment for services from another controller.

☐ We are processing the personal data as a result of a contract between us and the data subject.

☐ The data subjects are our employees.

☐ We make decisions about the individuals concerned as part of or as a result of the processing.

☐ We exercise professional judgement in the processing of the personal data.

☐ We have a direct relationship with the data subjects.

☐ We have complete autonomy as to how the personal data is processed.

☐ We have appointed one or more processors to process the personal data on our behalf.

Appendix 2 – Am I a joint controller?

You are likely to be a joint controller if you answer 'yes' to all of these questions in relation to a given set of processing.

☐ We have a common objective with others regarding the processing.

☐ We are processing the same personal data for the same purpose as another controller.

☐ We are using the same set of personal data (e.g., one database) for this processing as another controller.

☐ We have designed this process with another controller.

☐ We have common information management rules with another controller.

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 3 - Am I a processor?

You are likely to be a processor if you answer 'yes' to one or more of these questions in relation to a given set of processing.

☐ We are following instructions from someone else regarding the processing of personal data.

☐ We were given the personal data by a customer or similar third party or told what data to collect.

☐ We do not decide to collect personal data from individuals.

☐ We do not decide what personal data should be collected from individuals.

☐ We do not decide the lawful basis for the use of that data.

☐ We do not decide what purpose, or purposes, the data will be used for.

☐ We do not decide whether to disclose the data, or to whom.

☐ We do not decide how long to retain the data.

☐ We may make some decisions on how data is processed, but implement these decisions under a contract with someone else.

☐ We are not interested in the end result of the processing.

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 4 - Practical guidance controller, joint controller or processor?

The definition of a processor can be difficult to apply in the complexity of modern business relationships. We have outlined some examples to assist you in your assessment.

Processor examples

Example 1 (Processor)

A private company provides software to process the daily pupil attendance records of a state-maintained school. Using the software, the company gives attendance reports to the school.

The company's sole purpose in processing the attendance data is to provide this service to the school. The school sets the purpose – to assess attendance. The company has no need to retain the data after it has produced the report. It does not determine the purposes of the processing, it merely provides the processing service. This company is likely to be a processor.

Example 2 (Processor)

A bank hires an IT services firm to store archived data on its behalf – having ensured that the IT firm has given sufficient guarantees about the security of its systems and processes. The bank will still control how and why the data is used and determine its retention period. In reality, the IT services firm will use a great deal of its own technical expertise and professional judgement to decide how best to store the data in a safe and accessible way.

However, despite this freedom to take technical decisions, the IT firm is still not a controller in respect of the bank's data – it is a processor. This is because the bank retains exclusive control over the purpose for which the data is processed, if not exclusively over the manner in which the processing takes place.

Example 3 (Processor)

A marketing company sends promotional vouchers to a hairdresser's customers on the hairdresser's behalf. The marketing company is a processor for the hairdresser.

Example 4 (Processor)

The readers of a monthly science magazine receive a hard copy delivered to their home. Their subscriptions and the mailings are handled by a separate company at the publisher's request.

The company processing the subscriptions and arranging the mailing is a processor for the magazine publisher.

Example 5 (Processor)

An organisation uses a cloud service to store and analyse its data.

The organisation remains the controller and the cloud service provider is its processor.

Controller Examples

Example 1 (Controller)

A medical provider is sending envelopes containing patient data to another health provider and contracts a delivery service to deliver them. The delivery service is not processing the personal data contained in those envelopes. Although it is in physical possession of the envelopes, it has no idea what the envelopes contain and must not open them to access the content. For data protection purposes, the delivery service does not 'process' any personal data contained within those envelopes.

The hospital that chooses to use the delivery service is the controller responsible for the data contained in the envelopes. If the delivery service loses or misdirects an envelope containing highly sensitive personal data, for data protection purposes, the controller that sent it is responsible for that loss. So the sender should think carefully about the type of service that is most appropriate in the circumstances.

Controller and Processor examples

Example 1 (Controller and Processor)

An online retailer contracts a mail delivery service to deliver orders to customers. The customers can use a website to check the status of their order and track its delivery. The retailer will be the controller for any personal data inside the package. The delivery service will not be a controller or a processor for any personal data contained inside the package, as it has no control over or access to that data.

However, the delivery company will be processing some personal data (e.g. the name and address of the customer) in order to deliver the package and provide the tracking service. Whether it is a controller or a processor for the tracking element of the service will depend on who makes the decisions.

If the retailer makes the final decision on the tracking service to be provided and the delivery service merely follows the retailer's instructions, then the retailer will be the controller and the delivery service is likely to be a processor. But if the delivery company independently decides on the tracking service provided to individuals without the retailer's sign-off, it will be a controller.

Example 2 (Controller and Processor)

A specialist company provides software and data analysis to process the daily pupil attendance records of a school for an annual fee.

For the software provision the company is not a processor, but for the data analysis it is a processor for the school.

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.

Joint Controller example

Example 1 (Joint controller)

A fund administrator contracts a market-research company to carry out some research. The administrator's brief specifies its budget and that it requires a satisfaction survey of its main retail services based on the views of a sample of its customers across the EU. The administrator leaves it to the research company to determine sample sizes, interview methods and presentation of results.

The research company is processing personal data on the administrator's behalf, but it is also determining the information that is collected (what to ask the administrator's customers) and the manner in which the processing (the survey) will be carried out. It has the freedom to decide such matters as which customers to select for interview, what form the interview should take, what information to collect from customers and how to present the results.

This means the market-research company is likely to be a joint controller with the administrator regarding the processing of personal data to carry out the survey, even though the bank retains overall control of the data because it commissions the research and determines the purpose the data will be used for.