ORGANISATIONS

CONTROLLER OR **PROCESSOR**

digital **TOOLKIT**

Guidance for Organisations

JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

WWW.JERSEYOIC.ORG

Why is it Important to Distinguish Between Controllers and Processors?

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

- Your data protection obligations and how to meet them;
- Your responsibilities to individuals and the Jersey Office of the Information Commissioner and the penalties associated with non-compliance, such as administrative fines and other enforcement powers; and
- How you can work with other organisations to ensure you process personal data responsibly and respect individuals' rights.

Controllers (including joint controllers) have more obligations under the Data Protection (Jersey) Law 2018 than processors do, because they decide what personal data is collected from individuals and why, and exercise ultimate control over the data and how it is used.

Processors have obligations too and must be careful to only process personal data in line with the relevant controller's instructions.

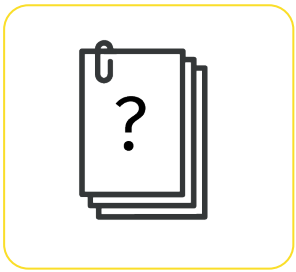
How do you determine whether you are a controller or processor?

It is important to remember that an organisation is not simply by its nature either a controller or a processor. Instead, the important thing to consider is 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.

You need to understand 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 all decisions that can only be taken by the controller as part of its overall control of the data processing operation. If you make any of these decisions determining the purposes and means of the processing, you are a controller. You can be a joint controller if you make those decisions jointly with another. If you are not the decision maker and you are only carrying out a function pursuant to someone else's orders (so, you are not unilaterally making any of the decisions set out above) you are a processor.



However, within the terms of its contract with the controller, a processor may decide:

- What IT systems or other methods to use to collect personal data;
- How to store the personal data;
- The details of the security measures to protect the personal data;
- How it will transfer the 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.

These lists are not exhaustive, but illustrate the differences between the controller's and the processor's roles. 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. However, it 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.

How does this apply in practice?

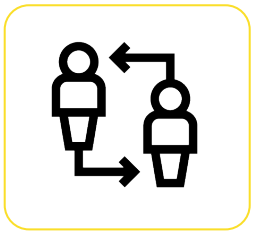
The definition of a processor can be difficult to apply in the complexity of modern business relationships. In practice, there is a scale of responsibility in how organisations work together to process personal data. The key is to determine each party's role in determining how and in what manner the data is processed as well as the degree of control over it.

At one extreme, one party (the client) will determine what personal data is to be processed and provide detailed processing instructions that the other party (the service provider) must follow. The service provider is tightly constrained in what it can do with the data and has no say at all over how it is processed. In this relationship the client is clearly the controller and the service provider is the processor.

However, it is far more common for a data controller to allow its processor a certain level of discretion over how the processing takes place using its own expertise.

Example

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 data 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

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.

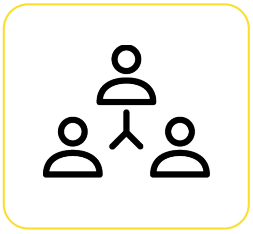
Example

A bank contracts a market-research company to carry out some research.
The bank'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 UK. The bank 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 bank's behalf, but it is also determining the information that is collected (what to ask the bank'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 a joint controller with the bank 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.

Example



A mail delivery service is contracted by a local hospital to deliver envelopes containing patients' medical records to other health service institutions. The delivery service is in physical possession of the envelopes but may not open them to access any of the personal data or other content they contain.

The delivery service will not process the personal data in the envelopes and packages it handles. It is in possession of the envelopes and packages but, as it cannot access their content, it cannot be said to be processing (it is not even 'holding') the personal data they contain. Indeed, the delivery service will have no idea as to whether the items they deliver contain personal data or simply other information.

This means that, regarding the content of the envelopes and packages it delivers, the delivery service is neither a controller in its own right nor a processor for the clients that use its services, because:

- *It does not exercise any control over the purpose for which the personal data enclosed in the items of mail entrusted to it is used; and*
- *It has no control over the content of the personal data entrusted to it.*

The controller (the hospital) that chooses to use the delivery service to transfer personal data is the party responsible for the data. If the delivery service loses a parcel containing highly sensitive personal data, the controller that sent the data is responsible for the loss. So, the controller will need to think carefully about the type of service that is most appropriate in the circumstances.

However, the delivery service will be a controller in its own right regarding any data it holds in connection with its provision of the delivery service. It will obviously be a controller regarding the HR data it processes about its own employees. In addition, to the extent that it records details of the delivery addresses of individuals (the name-and-address information on the items to be delivered), it will be a controller regarding that personal data. If the service arranges timed deliveries or tracking, then any personal data such as individual senders' and recipients' names and addresses it records for that purpose will be personal data for which the service is the controller.

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. 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 must 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.