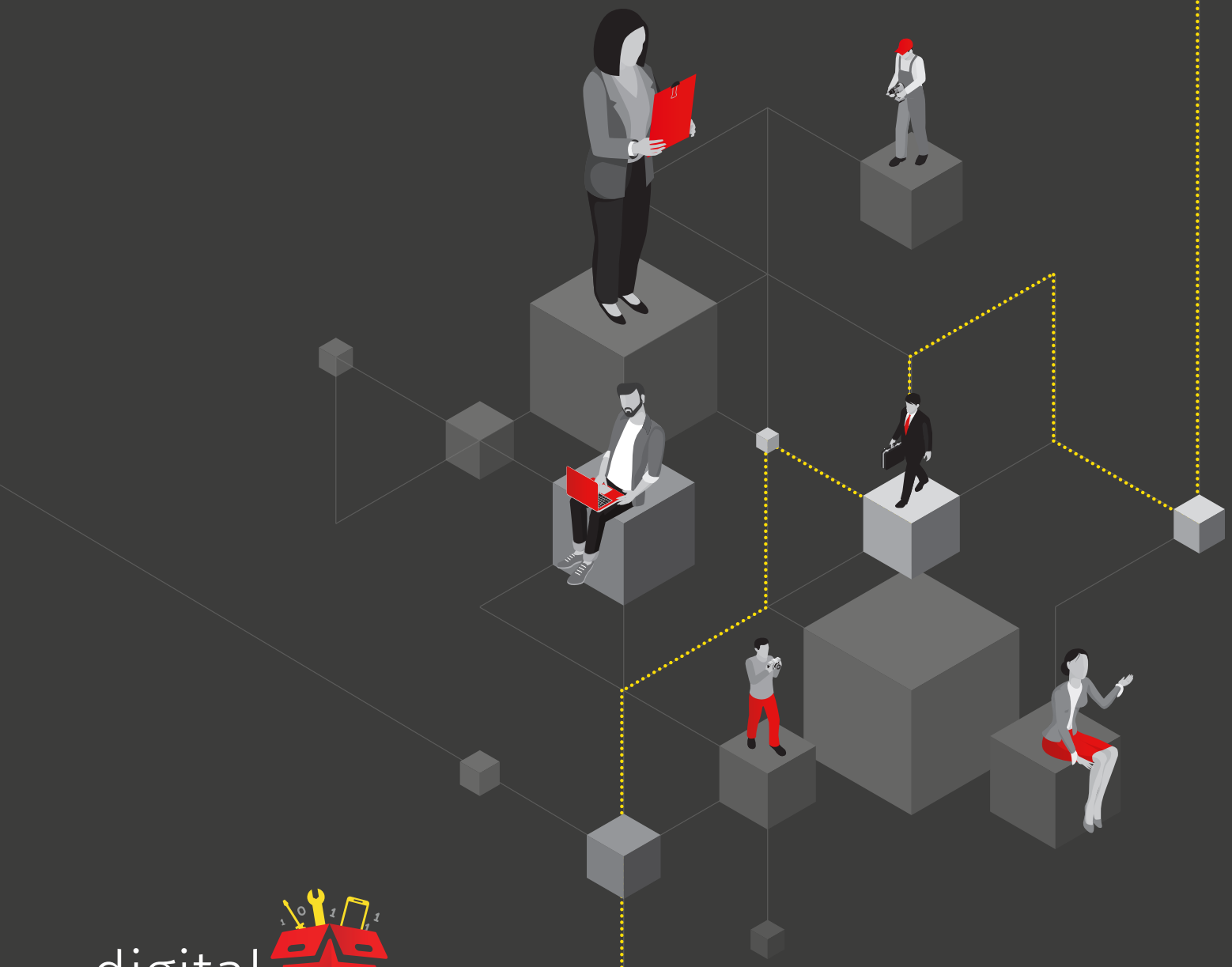
ORGANISATIONS

PERSONAL INFORMATION **AUDIT**



digital **TOOLKIT**

Guidance for Organisations

JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

WWW.JERSEYOIC.ORG

How do we Document our Processing Activities?

Most organisations must document their processing activities to some extent. Both **controllers and processors** have their own documentation obligations, but controllers need to keep more extensive records than processors.

Generally speaking, it is only organisations with 250 or more employees that must document all their processing activities UNLESS the particular organisation that has fewer than 250 employees is processing information that:

- Is likely to result in a risk to the rights and freedoms of data subjects;
- Is not occasional;
- Includes special category data or relates to criminal convictions or related security measures.

Even if you do not need to document some or all of your processing activities, the Jersey Office of the Information Commisioner (JOIC) urges you to do so as it is still good practice to do so. Keeping records on what personal data you hold, why you hold it and who you share it with will help you manage the data more effectively and comply with other aspects of the Data Protection (Jersey) Law 2018 (**DPJL**).

What do we need to document?

Article 14(3) of the DPJL says that a written record must be maintained, containing the following information:

- The name and contact details of the controller and any joint controller, representative of the controller or data protection officer;
- The purposes of the processing;
- A description of the categories of data subjects and personal data processed;
- A description of the recipients (if any) to whom the controller intends to, or may wish to, disclose the data;
- Where it is envisaged that data will be transferred to a third country or an international organisation, the name of that country or organisation, and in the case of transfers referred to in paragraph 9 of Schedule 3, the appropriate safeguards that are put in place;
- Where possible, the envisaged data retention periods for different categories of data;
- Where possible, a general description of the technical and organisational measures implemented in respect of the processed data.

How should we prepare?

A good way to start is by doing an information audit or data-mapping exercise to identify what personal data your organisation holds and where it is. It is important that people across your organisation are engaged in the process; this can help ensure nothing is missed when mapping the data your organisation processes and finding where information is. It is equally important to obtain senior management buy-in so that your mapping exercise is properly supported and well resourced.

What steps should we take next?

Once you have a basic idea of what personal data you have and where it is held, you will be in good position to begin documenting the information you must record under the DPJL. It is up to you how you do this, but we think these three steps will help you get there;

1. **Devise a questionnaire** – you can distribute this to the areas of the organisation you have identified as processing personal data. Use straightforward (jargon-free) questions in plain English that will prompt answers to the areas requiring documentation.

   Example questions

   - Why do you use personal data?
   - Who do you hold information about?
   - What information do you hold about them?
   - Who do you share it with?
   - How long do you hold it for?
   - How do you keep it safe?

2. **Meet directly with key business functions** – this will help you gain a better understanding of how certain parts of your organisation use data.

   Example business functions

   - IT staff can help answer questions about technical security measures;
   - Information governance staff should be able to provide information on retention periods;
   - Legal and compliance staff may hold details of any data-sharing arrangements.

3. **Locate and review policies, procedures, contracts and agreements** – as well as feeding directly into the documentation exercise, this can help you compare and contrast intended and actual data processing activities.

   Example documents

   - Privacy policies;
   - Data protection policies;
   - Data retention policies;
   - Data security policies;
   - System use procedures;
   - Data processor contracts;
   - Data sharing agreements.

How should we document our findings?

The documentation of your processing activities must be in writing; this can be in paper or electronic form. Generally, most organisations will benefit from maintaining their documentation electronically so they can easily add to, remove, and amend it as necessary.

TIP

Paper documentation may be adequate for very small organisations whose processing activities rarely change.

However, you choose to document your organisation's processing activities, it is important that you do it in a granular and meaningful way. For instance, you may have several separate retention periods, each specifically relating to different categories of personal data. Equally it is likely that the organisations you share personal data with differ depending on the type of people you hold information on and your purposes for processing the data. The record of your processing activities needs to reflect these differences.

Example - would meet the DPJL documentation requirements:

Purposes of processing	Categories of individuals	Categories of personal data
Staff administration	Employees	Contact details
		Financial details
	Emergency contacts	Contact details
Customer orders	Customers	Contact details
		Financial details
		IP address
	Suppliers	Contact details
		Financial details
		Location
Marketing	Customers	Contact details
		Lifestyle information
	Clients	Contact details

What should we document first?

Start with the broadest piece of information about a particular processing activity, then gradually narrow the scope.

Controllers; it makes sense for controllers to begin with a business function – e.g. HR, Sales, Customer Services. Although the DPJL does not require you to document this information, focusing on each function of your business, one at a time, will help to give your record of processing activities a logical structure. Each business function is likely to have several different purposes for processing personal data, each purpose will involve several different categories of individuals, and in turn those categories of individuals will have their own categories of personal data and so on.

Processors; although you have less information to document as a processor, it still helps to adopt a 'broad to narrow' approach. Start with the controller you are processing personal data for. There may be several different categories of processing you carry out for each controller, and in turn different types of international transfers, security measures and so on.

Documentation using this type of approach should help you create a complete and comprehensive record of your processing activities within which you document the different types of information in a granular way and meaningfully link them together.

What if we have an existing documentation method?

In addition to data protection, some organisations (even small ones) are often subject to several other regulations that have their own documentation obligations, particularly in sectors such as insurance and finance. If your organisation is subject to such regulatory requirements, you may already have an established data governance framework in place that supports your existing documentation procedures; it may even overlap with the DPJL's record-keeping requirements. If so, the DPJL does not prohibit you from combining and embedding the documentation of your processing activities with your existing record-keeping practices. But you should be careful to ensure you can deliver all the requirements of Article 14, if necessary by adjusting your data governance framework to account for them.

Do we need to update our record of processing activities?

Keeping a record of your processing activities is not a one-off exercise; the information you document must reflect the current situation as regards the processing of personal data. You should treat the record as a living document that you update as and when necessary. This means you should conduct regular reviews of the information you process to ensure your documentation remains accurate and up to date.

We have created a template processing record that will help you comply with the requirements of Article 14.