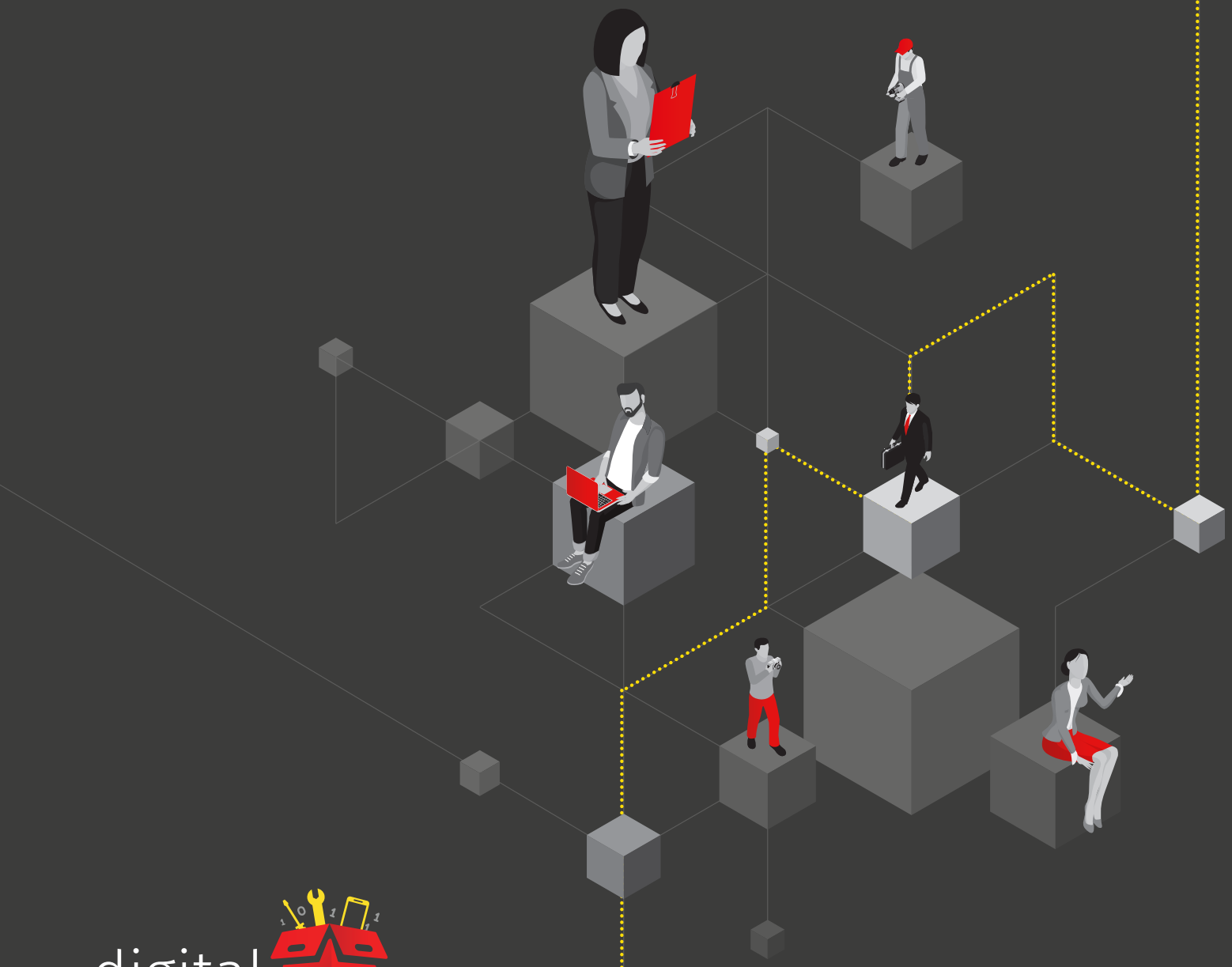
ORGANISATIONS

ACCOUNTABILITY AND GOVERNANCE



digital TOOLKIT

Guidance for Organisations

JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

WWW.JERSEYOIC.ORG

Accountability and Governance

Responsibility for data protection comes from the top of your organisation, it is a senior management and board matter.

Accountability is one of the data protection principles - you are responsible for complying with the Data Protection (Jersey) Law 2018 (**DPJL**) and you must be able to evidence your compliance.

Accountability is not just about being answerable to the regulator however; you must also demonstrate your compliance to the individuals whose data your process. Amongst other things, individuals have the right to be informed about what personal data you collect, why you use it and who you share it with. Additionally, if you use techniques such as artificial intelligence and machine learning to make decisions about people, in certain cases individuals have the right to hold you to account by requesting explanations of those decisions and contesting them. You therefore need to find effective ways to provide information to people about what you do with their personal data, and explain and review automated decisions.

The obligations that accountability places on you are ongoing – you cannot simply sign off a particular processing operation as 'compliant' and move on. You must review the measures you implement at appropriate intervals to ensure that they remain appropriate and effective. You should update measures that are no longer fit for purpose. If you regularly change what you do with personal data, or the types of information that you collect, you should review and update your measures frequently, remembering to document what you do and why. You need to tell individuals about any changes.

At a Glance

- You need to put in place appropriate technical and organisational measures to meet the requirements of accountability;
- There are a number of measures that you can, and in some cases must, take including:
  - Adopting and implementing data protection policies;
  - Taking a 'data protection by design and default' approach;
  - Putting written contracts in place with organisations that process personal data on your behalf;
  - Maintaining a record of your processing activities;
  - Implementing appropriate security measures;
  - Recording and, where necessary, reporting personal data breaches;
  - Carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests;
  - Appointing a data protection officer;
  - Adhering to any relevant codes of conduct and signing up to certification schemes.
- Accountability obligations are ongoing. You must review and, where necessary, update the measures you put in place.

If you implement a privacy management framework this can help you embed your accountability measures and create a culture of privacy across your organisation.

Being accountable can help you to build trust with individuals and may help you mitigate enforcement action.

What is Accountability?

There are two key elements.

1. The accountability principle makes it clear that you are responsible for complying with the DPJL.
2. You must be able to demonstrate your compliance.

Why is accountability important?

Taking responsibility for what you do with personal data, and demonstrating the steps you have taken to protect people's rights not only results in better legal compliance, it also offers you a competitive edge.

> *Accountability is a real opportunity for you to show, and prove, how you respect people's privacy. This can help you to develop and sustain people's trust.*

Furthermore, if something does go wrong, then being able to show that you actively considered the risks and put in place measures and safeguards can help you provide mitigation against any potential enforcement action. On the other hand, if you can't show good data protection practices, it may leave you open to enforcement action by the regulator, civil court claims brought by affected data subjects and reputational damage.

What do we need to do?

Accountability is not a box-ticking exercise. Being responsible for compliance with the DPJL means that you need to be proactive and organised about your approach to data protection, while demonstrating your compliance means that you must be able to evidence the steps you take to comply and show that you have appropriate technical and organisational measures in place that ensure and demonstrate that you are compliant with the law.

To achieve this, if you are a larger organisation you may choose to put in place a privacy management framework. This can help you create a culture of commitment to data protection, by embedding systematic and demonstrable compliance across your organisation. Amongst other things, your framework should include:

- Robust program controls informed by the requirements of the DPJL;
- Appropriate reporting structures;
- Assessment and evaluation procedures.

If you are a smaller organisation you will still need to be able to demonstrate your compliance with the DPJL but this will likely be on a smaller scale than for larger organisations. The measures you put in place need to be appropriate and proportionate for the size of your organisation.

Article 14(1) of the DPJL says that you must implement technical and organisational measures to ensure, and demonstrate, compliance with the DPJL. The measures should be risk-based and proportionate having regard to;

- The nature, scope, context and purposes of processing;
- The risk and likelihood of prejudice to the rights of data subjects;
- Best practices in technical and organisational measures;
- The state of technological development;
- The costs of implementation.

Amongst other things you should;

- Ensure a good level of understanding and awareness of data protection amongst your staff;
- Implement comprehensive but proportionate policies and procedures for handling personal data;
- Keep records of what you do and why.

Should we implement data protection policies?

For many organisations, putting in place relevant policies is a fundamental part of their approach to data protection compliance. The DPJL explicitly says where proportionate, implementing data protection policies is one of the measures you can take to ensure, and demonstrate, compliance.

What you have policies for, and their level of detail, depends on what you do with personal data. If, for instance, you handle large volumes of personal data, or particularly sensitive information such as **special category data**, then you should take greater care to ensure that your policies are robust and comprehensive.

As well as drafting data protection policies, you should also be able to show that you have implemented and adhered to them. This could include awareness raising, training, monitoring and audits – all tasks that your data protection officer can undertake.

Should we adopt a 'data protection by design and default' approach?

Privacy by design has long been seen as a good practice approach when designing new products, processes and systems that use personal data. Under the heading 'data protection by design and by default', the DPJL legally requires you to take this approach.

Data protection by design and default is an integral element of being accountable. It is about embedding data protection into everything you do, throughout all your processing operations. The DPJL suggests measures that may be appropriate such as minimising the data you collect, applying **pseudonymisation** techniques, and improving security features.

Integrating data protection considerations into your operations helps you to comply with your obligations, while documenting the decisions you take (including in data protection impact assessments – see below) demonstrates this.

Do we need to use contracts?

Whenever a **controller uses a processor** to handle personal data on their behalf, it needs to put in place a written contract that sets out each party's responsibilities and liabilities.

Contracts must include certain specific terms as a minimum, such as requiring the processor to take appropriate measures to ensure the security of processing and obliging it to assist the controller in allowing individuals to exercise their rights under the DPJL.

Using clear and comprehensive contracts with your processors helps to ensure that everyone understands their data protection obligations.

What documentation should we maintain?

Under Article 14(3) of the DPJL, most organisations are required to maintain a record of their processing activities, covering areas such as processing purposes, data sharing and retention.

Documenting this information allows you to take stock of what you do with personal data. Knowing what information you have, where it is and what you do with it makes it much easier for you to comply with other aspects of the DPJL such as making sure that the information you hold about people is accurate and secure and that you aren't actually collecting more than you need for your purposes.

As well as your record of processing activities under Article 14, you also need to document other things to show your compliance with the DPJL. For instance, you need to keep records of consent and any personal data breaches that occur.

What security measures should we put in place?

The DPJL repeats the requirement to implement technical and organisational measures to comply with the DPJL in the context of security. It says that these measures should ensure a level of security appropriate to the risks should that information be compromised. What is the worst that could happen?

You need to implement security measures if you are handling any type of personal data, but what you put in place depends on your particular circumstances. You need to ensure the confidentiality, integrity and availability of the systems and services you use to process personal data.

Amongst other things, this may include information security policies, access controls, security monitoring, and recovery plans.

Should we carry out data protection impact assessments (DPIAs)?

A **DPIA** is an essential accountability tool and a key part of taking a data protection by design approach to what you do. It helps you to identify and minimise the data protection risks of any new projects you undertake.

A DPIA is a legal requirement before carrying out processing likely to result in high risk to individuals' interests.

When done properly, a DPIA helps you assess how to comply with the requirements of the DPJL, while also acting as documented evidence of your decision-making and the steps you took.

How do we record and report personal data breaches?

You must report certain types of personal **data breach** to the relevant supervisory authority (for Jersey, this is the Jersey Office of the Information Commissioner (JOIC) and, in some circumstances, to the affected individuals as well.

Additionally, the DPJL says that you must keep a r**ecord of any personal data breaches**, regardless of whether you need to report them or not.

You need to be able to detect, investigate, report (both internally and externally) and document any breaches. Having robust policies, procedures and reporting structures helps you do this and identify any weak spots in your organisation (for example, certain departments or employees).

Checklist

- [ ] We take responsibility for complying with the DPJL, at the highest management level and throughout our organisation.
- [ ] We keep evidence of the steps we take to comply with the DPJL.

We put in place appropriate technical and organisational measures, such as;

- [ ] Adopting and implementing data protection policies (where proportionate);
- [ ] Taking a 'data protection by design and default' approach - putting appropriate data protection measures in place throughout the entire lifecycle of our processing operations;
- [ ] Putting written contracts in place with organisations that process personal data on our behalf;
- [ ] Maintaining documentation of our processing activities;
- [ ] Implementing appropriate security measures;
- [ ] Recording and, where necessary, reporting personal data breaches;
- [ ] Carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests;
- [ ] Appointing a data protection officer (where necessary);
- [ ] Adhering to relevant codes of conduct and signing up to certification schemes (where possible).

- [ ] We review and update our accountability measures at appropriate intervals.