ORGANISATIONS

THE ELEMENTS OF A GOOD **DATA PROTECTION POLICY**

digital **TOOLKIT**

Guidance for Organisations

JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

WWW.JERSEYOIC.ORG

What are the Elements of a Good Data Protection Policy?

The following topics should be included in a data protection policy;

- Reflects all elements of the data protection principles;
- Data Protection Lead/Officer;
- Know your personal data;
- Appropriate policies and protocols;
- Training & awareness;
- Periodic review;
- Senior management and executive buy in.

Whatever your business, it's essential that your company has formal data protection policies and procedures in place so that you are able to demonstrate your compliance with the Data Protection (Jersey) Law 2018 (DPJL).

By implementing a robust data protection policy and framework this can help you embed your accountability measures and create a culture of privacy throughout your organisation, regardless of size or organisation type.

Fostering an active data protection culture can help you to build trust with staff and customers. It will help your reputation and may help you mitigate the effects of any enforcement action. Accountability obligations are ongoing. You must review and, where necessary, update the measures you have in place.

Your data protection policy should reflect the obligations bestowed on you by the DPJL which is based around six principles of 'good information handling' (the Principles).

These principles give people (the data subjects) specific rights in relation to their personal information and place certain obligations on those organisations that are responsible for processing it.

They are set out at Article 8 DPJL:

- **FAIR, LAWFUL AND TRANSPARENT PROCESSING:** Personal data are to be processed lawfully, fairly and in a transparent manner in relation to the data;
- **PURPOSE LIMITATION:** Personal data must be collected for specified, explicit and legitimate purposes and once collected, not further processed in a manner incompatible with those purposes;
- **EXCESSIVE DATA COLLECTION:** Personal data collected must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- **ACCURACY OF DATA:** Personal data must be accurate and, where necessary, kept up to date, with reasonable steps being taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- **STORAGE LIMITATION:** Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed;
- **DATA SECURITY, INTEGRITY AND CONFIDENTIALITY:** Personal data must be processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The Principles are at the core of the responsibilities placed upon controllers and processors. Whilst compliance with each Principle must be met, they are inextricably linked and therefore should not be read in isolation. Your policy needs to explain how your organisation will comply with the principles above.

TIP

The organisation's data protection policy should embrace

- Appropriate technical and organisational measures to meet the requirements of accountability;
- Adopting and implementing data protection policies;
- A 'data protection by design' approach;
- Written contracts where appropriate;
- A record of your processing activities;
- How you implement appropriate security measures;
- Data breach plan to record and, where necessary, report personal data breaches;
- Identifying a data protection lead.

Your policy should be clear and set out information in a way that is easy for your employees to understand and follow.