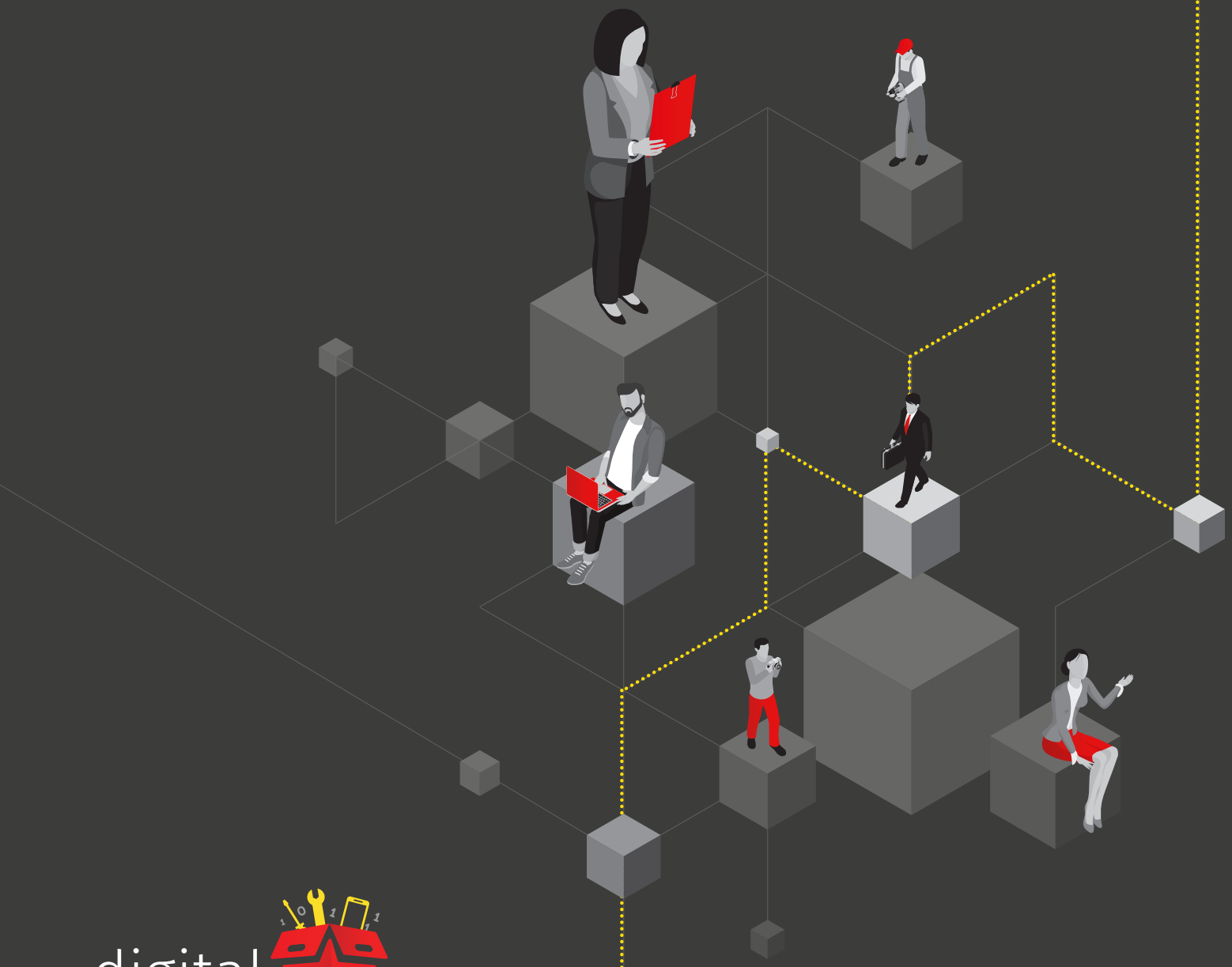
ORGANISATIONS

STORAGE AND **RETENTION**



digital **TOOLKIT**

Guidance for Organisations

JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

WWW.JERSEYOIC.ORG

Storage and Retention

The fifth data protection principle (Art.8(1)(e) of the DPJL) requires personal data must not be kept for longer than is necessary for the purposes for which it is being processed.

Data protection principles

'A controller must ensure that the processing of personal data in relation to which the controller is the controller complies with the data protection principles, namely that data are;

- Processed lawfully, fairly and in a transparent manner in relation to the data ('lawfulness, fairness and transparency');
- Collected for specified, explicit and legitimate purposes and once collected, not further processed in a manner incompatible with those purposes ('purpose limitation');
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- 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 ('accuracy');
- 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 ('storage limitation');
- 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 ('integrity and confidentiality').

Why is storage limitation important?

Ensuring that you erase or anonymise personal data when you no longer need it will reduce the risk that it becomes irrelevant, excessive, inaccurate or out of date. Apart from helping you to comply with the data minimisation and accuracy principles, this also reduces the risk that you will use such data in error – to the detriment of all concerned.

Personal data held for too long will, by definition, be unnecessary. You are unlikely to have a lawful basis for retention.

From a more practical perspective, it is inefficient to hold more personal data than you need, and there may be unnecessary costs associated with storage and security.

Remember that you must also respond to subject access requests for any personal data you hold. This may be more difficult if you are holding old data for longer than you need.

Good practice around storage limitation - with clear policies on retention periods and erasure - is also likely to reduce the burden of dealing with queries about retention and individual requests for erasure.

At a glance

- You must not keep personal data for longer than you need it.
- You need to think about – and be able to justify – how long you keep personal data. This will depend on why you are holding the data.
- You need a policy (or some other mechanism) setting standard **retention** periods wherever possible, to comply with documentation requirements.
- You should also periodically review the data you hold, and erase or anonymise it when you no longer need it. This will help you ensure that the data you hold is not inaccurate, out of date or irrelevant.
- You must carefully consider any challenges to your retention of data. Individuals have a right to request erasure of the data if you no longer need it.
- At the end of the retention period, unless there is a reason for keeping it, personal data should be deleted. Some companies may use automated systems which delete data after a certain period where they hold a number of records of the same type of data.
- You can keep personal data for longer if you are only keeping it for archiving, statistical, scientific or historical research. In particular, organisations should not retain personal data in case it is needed in the future, or if there is a small possibility that it might be needed (not 'just in case').
- Personal data should only be archived where you need to hold the information for some reason, otherwise it should be deleted. When personal data is deleted at the end of the retention period, this should also be deleted from any back-up. When considering compliance with the Data Protection principles, you should think about;
    - The value of the personal data being retained, both in the future and at the current date;
    - The purpose for which the personal data was obtained and the nature of the personal data;
    - What the costs, risks and liabilities are that are associated with retaining the information;
    - How easy it is to ensure that the personal data is kept up to date and accurate;
    - If there are any legal or regulatory requirements;
    - If there are any sector specific requirements and agreed practices.

Checklist

- [ ] We know what personal data we hold and why we need it;
- [ ] We carefully consider and can justify how long we keep personal data;
- [ ] We have a policy with standard retention periods where possible, in line with documentation obligations;
- [ ] We regularly review our information and erase or anonymise personal data when we no longer need it;
- [ ] We have appropriate processes in place to comply with individuals' requests for erasure under 'the right to be forgotten';
- [ ] We clearly identify any personal data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes.

Jersey Office of the Information Commissioner, 2nd Floor, 5 Castle Street, St Helier, Jersey JE2 3BT
Telephone number: +44 (0) 1534 716530 | **Email:** enquiries@jerseyoic.org