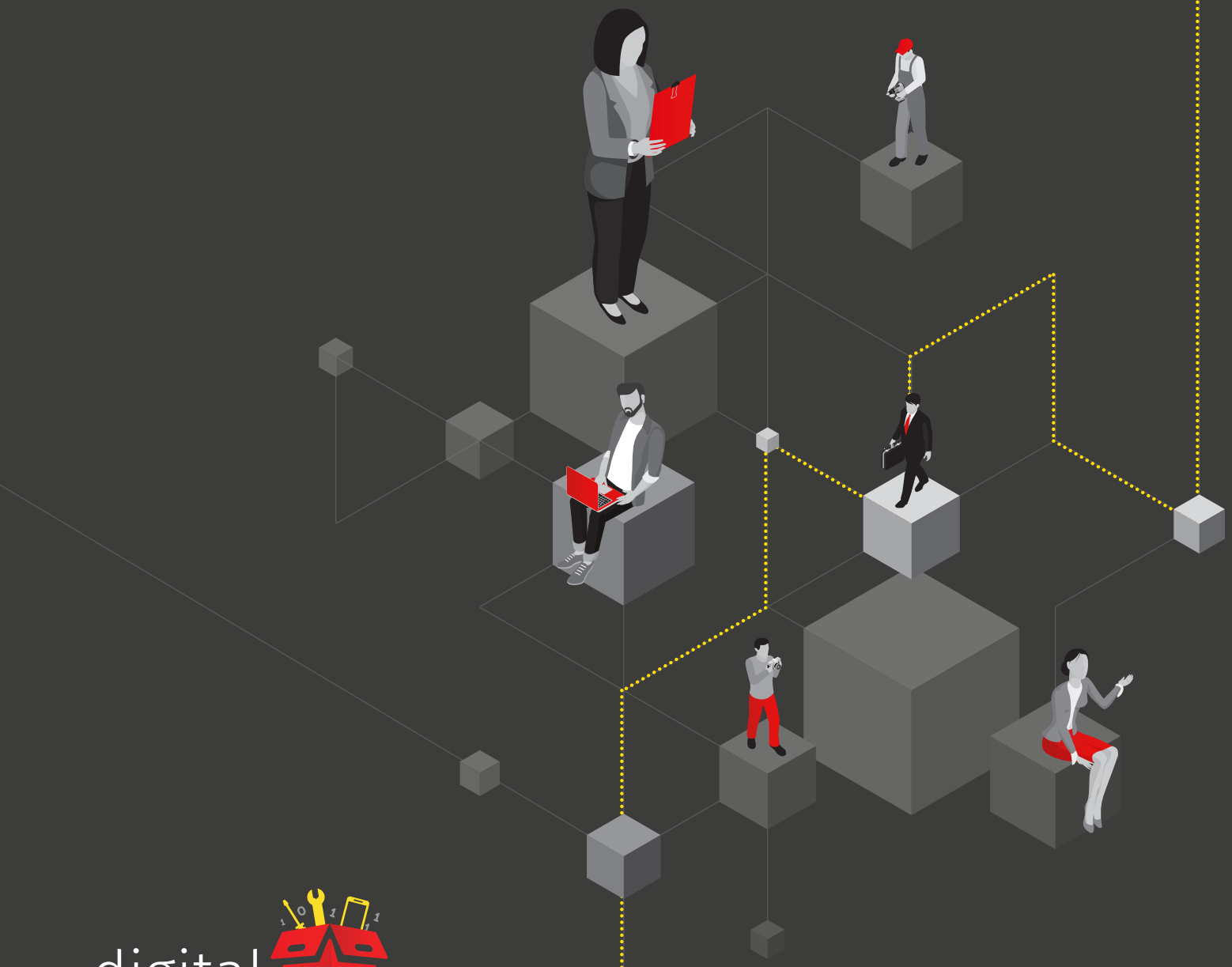
ORGANISATIONS

DO WE NEED A **RETENTION POLICY**



digital **TOOLKIT**

Guidance for Organisations

JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

WWW.JERSEYOIC.ORG

Do we Need a Retention Policy?

Retention policies or retention schedules list the types of record or information you hold, what you use it for, and how long you intend to keep it. They help you establish and document standard retention periods for different categories of personal data and explain to individuals why you are keeping information and how long for.

A retention schedule will form part of a broader suite of internal measures and documents about how an organisation deals with data protection matters.

You need to establish and document the applicable retention periods for all the different categories of personal information you process, as per (Article 14(3)(f) of the Data Protection (Jersey) Law 2018 (**DPJL**)).

It is also advisable to have a system for ensuring that your organisation keeps to these retention periods in practice, and for reviewing retention at appropriate intervals. Your policy must also be flexible enough to allow for early deletion if appropriate. For example, if you are not actually using a record, you should reconsider whether you actually need to retain it at all or for as long as previously envisaged.

If you don't have a retention policy (or if it doesn't refer to all of the personal data you hold), you must still regularly review the data you hold, and delete or anonymise anything you no longer need. (This is so that you can demonstrate compliance with principle 8(1)(c) of the (DPJL) and show that you are only processing data that is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').

How long do we need to keep information for?

The DPJL does not dictate how long you should keep personal data. It is up to you to justify this, based on your purposes for processing. You are in the best position to judge how long you need it and to be able to explain why.

You should consider your stated purposes for processing the personal data. You can keep it as long as one of those purposes still applies, but you should not keep data indefinitely 'just in case', or if there is only a small possibility that you may use it in the future.

You must also be able to justify why you need to keep personal data in a form that permits identification of individuals. If you do not need to identify individuals, you should anonymise the data so that identification is no longer possible.

You should consider any legal or regulatory requirements. There are various legal requirements and professional guidelines about keeping certain kinds of records – such as information needed for income tax and audit purposes, or information on aspects of health and safety. If you keep personal data to comply with a requirement like this, you will not usually be considered to have kept the information for longer than necessary but the burden is on you to justify why you have kept information for a particular length of time.

You must remember to take a proportionate approach, balancing your needs with the impact of retention on individuals' privacy. Don't forget that your retention of the data must also always be fair and lawful.

EXAMPLE

An employer should review the personal data it holds about an employee when they leave the organisation's employment. It will need to retain enough data to enable the organisation to deal with, for example, providing references or pension arrangements. However, it should delete personal data that it is unlikely to need again from its records – such as the employee's emergency contact details, previous addresses, or death-in-service beneficiary details.

EXAMPLE

A bank may need to retain images from a CCTV system installed to prevent fraud at an ATM machine for several weeks, since a suspicious transaction may not come to light until a victim gets their bank statement. In contrast, a pub may only need to retain images from their CCTV system for a short period because incidents will come to light very quickly. (However, if a crime is reported to the police, the pub will need to retain images until the police have time to collect them.)

EXAMPLE

A tracing agency holds personal data about a debtor so that it can find that individual on behalf of a creditor. Once it has found the individual and reported to the creditor, there may be no need to retain the information about the debtor – the agency should remove it from their systems unless there are good reasons for keeping it. Such reasons could include if the agency has also been asked to collect the debt, or because the agency is authorised to use the information to trace debtors on behalf of other creditors.

You should consider whether you need to keep a record of a relationship with the individual once that relationship ends. You may not need to delete all personal data when the relationship ends. You may need to keep some information so that you can confirm that the relationship existed – and that it has ended – as well as some of its details.

EXAMPLE

A business receives a notice from a former customer requiring it to stop processing the customer's personal data for direct marketing. It is appropriate for the business to retain enough information about the former customer for it to stop including that person in future direct marketing activities.

You should consider whether you need to keep information to defend possible future legal claims. However, you could still delete information that could not possibly be relevant to such a claim. Unless there is some other reason for keeping it, personal data should be deleted when such a claim could no longer arise (e.g. once the relevant legal time period for bringing a claim has passed).

EXAMPLE

An employer receives several applications for a job vacancy. Unless there is a clear business reason for doing so, the employer should not keep recruitment records for unsuccessful applicants beyond the statutory period in which a claim arising from the recruitment process may be brought (e.g. a discrimination claim).

You must also be able to justify why you need to keep personal data in a form that permits identification of individuals. If you do not need to identify individuals, you should anonymise the data so that identification is no longer possible.

You should consider any legal or regulatory requirements. There are various legal requirements and professional guidelines about keeping certain kinds of records – such as information needed for income tax and audit purposes, or information on aspects of health and safety. If you keep personal data to comply with a requirement like this, you will not usually be considered to have kept the information for longer than necessary but the burden is on you to justify why you have kept information for a particular length of time.

You must remember to take a proportionate approach, balancing your needs with the impact of retention on individuals' privacy. Don't forget that your retention of the data must also always be fair and lawful.

When should we review our retention?

You should review whether you still need personal data at the end of any standard retention period, and erase or anonymise it unless there is a clear justification for keeping it for longer. Automated systems can flag records for review, or delete information after a pre-determined period. This is particularly useful if you hold many records of the same type.

It is also good practice to review your retention of personal data at regular intervals before this, especially if the standard retention period is lengthy or there is potential for a significant impact on individuals.

TIP

If you don't have a set retention period for the personal data, you must regularly review whether you still need it.

However, there is no firm rule about how regular these reviews must be. Your resources may be a relevant factor here, along with the privacy risk to individuals. The important thing to remember is that you must be able to justify your retention and how often you review it.

Individuals have the right to request erasure of personal data that you no longer need for your specified purposes and you must carry out that request without undue delay unless one of the exemptions at Article 32(3) applies.

What should we do with personal data that we no longer need?

You can either erase (delete) it, or anonymise it.

You need to remember that there is a significant difference between permanently deleting personal data, and taking it offline. If personal data is stored offline, this should reduce its availability and the risk of misuse or mistake. However, you are still processing personal data. You should only store it offline (rather than delete it) if you can still justify holding it. You must be prepared to respond to subject access requests for personal data stored offline, and you must still comply with all the other principles and rights.

The word 'deletion' can mean different things in relation to electronic data, and we recognise it is not always possible to delete or erase all traces of the data. The key issue is to ensure you put the data beyond use. If it is appropriate to delete personal data from a live system, you should also delete it from any back-up of the information on that system.