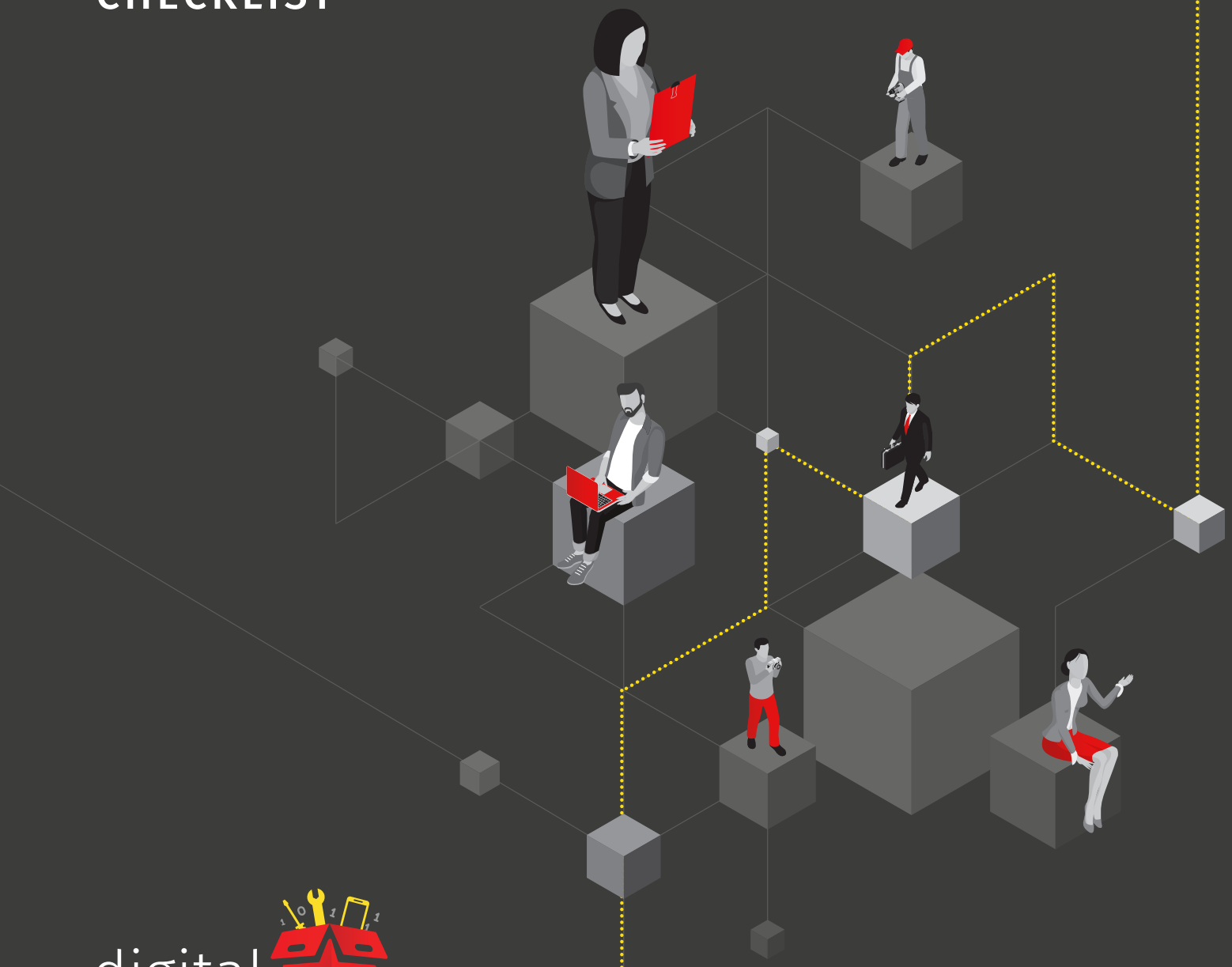
ORGANISATIONS

PERSONAL DATA BREACHES

CHECKLIST



digital TOOLKIT

Guidance for Organisations

This document is purely for guidance and does not constitute legal advice or legal analysis. It is intended as a starting point only, and organisations may need to seek independent legal advice when renewing, enhancing or developing their own processes and procedures or for specific legal issues and/or questions.

JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

WWW.JERSEYOIC.ORG

At a Glance

The Data Protection (Jersey) Law 2018 ('**DPJL**') introduced a duty on all organisations to report certain types of personal data breach to the Jersey Office of the Information Commissioner ('the **JOIC**'). You must do this within 72 hours of becoming aware of the breach, where feasible.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.

You should ensure you have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals.

You must also keep a record of any personal data breaches, regardless of whether you are required to notify.

Checklists

Preparing for a personal data breach

- [ ] We know how to recognise a personal data breach;
- [ ] We understand that a personal data breach isn't only about loss or theft of personal data;
- [ ] We have prepared a response plan for addressing any personal data breaches that occur;
- [ ] We have allocated responsibility for managing breaches to a dedicated person or team;
- [ ] Our staff know how to escalate a security incident to the appropriate person or team in our organisation to determine whether a breach has occurred.

Responding to a personal data breach

- [ ] We have in place a process to assess the likely risk to individuals as a result of a breach;
- [ ] We know who is the relevant supervisory authority for our processing activities;
- [ ] We have a process to notify the JOIC of a breach within 72 hours of becoming aware of it, even if we do not have all the details yet;
- [ ] If we are unsure what and how to report a breach to the JOIC we will contact the JOIC to ask;
- [ ] We will have a process to inform affected individuals about a breach when it is likely to result in a high risk to their rights and freedoms;
- [ ] We know we must inform affected individuals without undue delay;

- [ ] We know what information about a breach we must provide to individuals, and that we should provide advice to help them protect themselves from its effects;
- [ ] We document all breaches, even if they don't all need to be reported.

What is a personal data breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Example

Personal data breaches can include:

- Access by an unauthorised third party;
- Deliberate or accidental action (or inaction) by a controller or processor;
- Sending personal data to an incorrect recipient;
- Computing devices containing personal data being lost or stolen;
- Alteration of personal data without permission; or
- Loss of availability of personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

The DPJL makes clear that when a security incident takes place, you should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the JOIC if required.

What breaches do we need to notify the JOIC about?

When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then you must notify the JOIC; if it's unlikely then you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it.

In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals.

This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. You need to assess this case by case, looking at all relevant factors.

What role do processors have?

If your organisation uses a data processor, and this processor suffers a breach, then under Article 22(1)(g) it must inform you without undue delay as soon as it becomes aware.

Example

Your organisation (the controller) contracts an IT services firm (the processor) to archive and store customer records. The IT firm detects an attack on its network that results in personal data about its clients being unlawfully accessed. As this is a personal data breach, the IT firm promptly notifies you that the breach has taken place. You in turn notify the JOIC.

This requirement allows you to take steps to address the breach and meet your breach-reporting obligations under the DPJL.

For more information check out the **breach section** on our website.

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