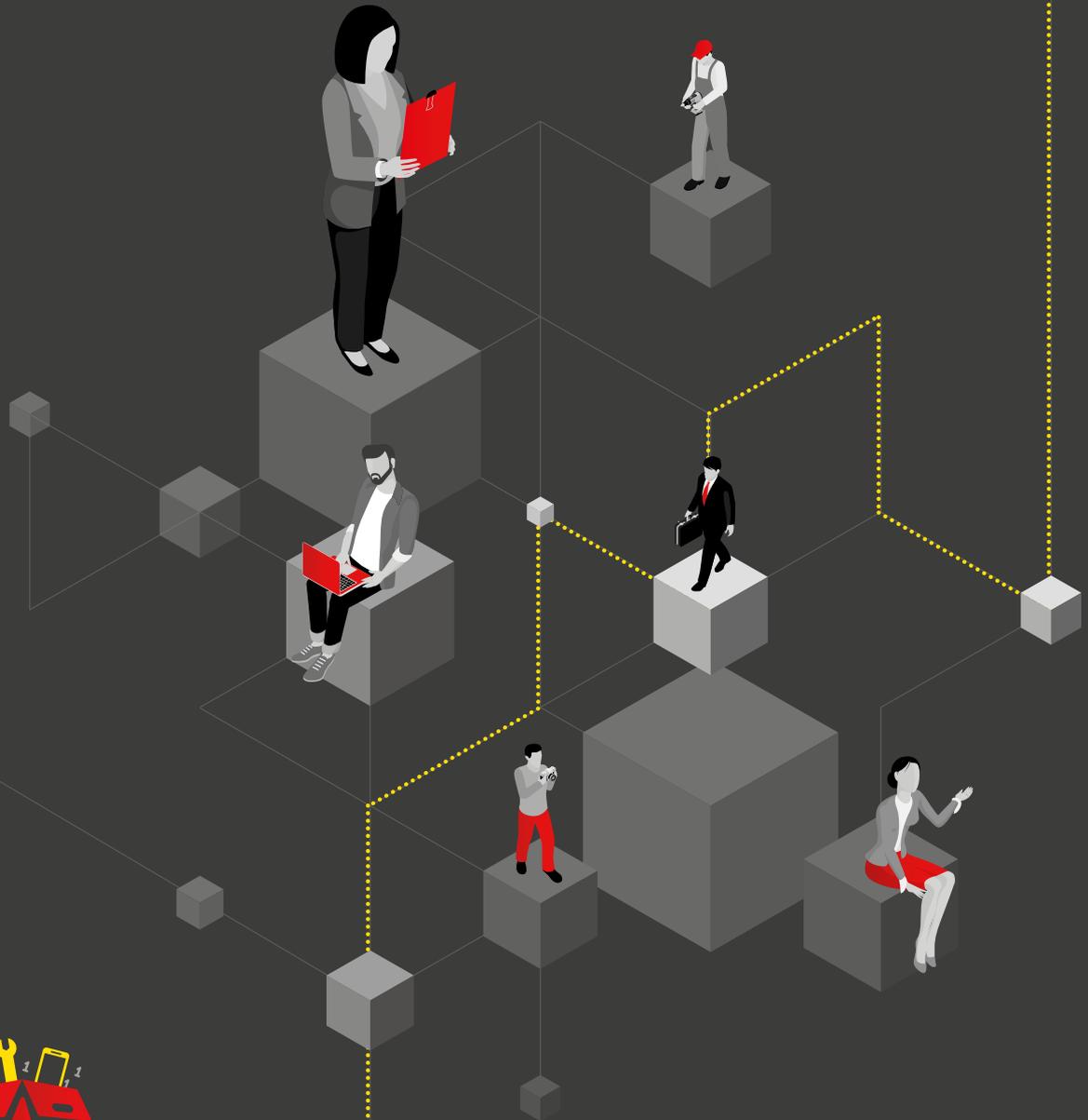




NON-EXECUTIVE

DATA PROTECTION 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



Non-Executive Directors Data Protection Toolkit

Non-executive directors (NED) are responsible for providing independent oversight, constructive challenge to executive directors and holding management to account. Data protection is part of the governance and risk management program responsibility of the board.

Data Protection legislation is in place to help ensure, that when it comes to our **personal data**, all of us are provided with appropriate legal protections and remedies in today's highly digitised world. It is a positive concept, which seeks to hold organisations entrusted with our **personal information** accountable and to set standards for how that information is used.

While good data protection regulation should promote economic growth, its primary purpose is to recognise that privacy is a fundamental human right that is currently under increasing threat. Rapidly advancing technology has increased privacy risks exponentially. Make sure you understand your obligations under the **Data Protection (Jersey) Law 2018 (DPJL)** and how it helps you maintain client and staff trust.

The DPJL places direct **obligations** relating to the processing of personal information on business and organisations. The DPJL states that an organisation can only process personal information where certain conditions are satisfied. For instance, the processing should be fair, transparent, for a specified and legitimate purpose, and limited to the personal information necessary to fulfil this purpose. Information must not be kept for longer than needed.

The DPJL is based around **six principles** of 'good information handling'. These principles place certain obligations on those organisations that are responsible for processing it and set the standards for how personal data must be handled.

The DPJL applies to the public, private, charity and not-for-profit sectors and all organisations that process personal data must be **registered** with the Authority (and pay a fee where required).

The DPJL applies to '**controllers**' and '**processors**'. A controller determines the purposes and means of processing personal data and a processor is responsible for processing personal data on behalf of a controller and in accordance with the controller's specific, written instructions.

Both data controllers and processors are subject to a number of statutory duties under the DPJL. This guidance sets out those general duties as part of an overall principle of accountability, helping organisations fully understand their obligations, as well as to promote good practice.



The NED Data Protection Checklist

To help you navigate and understand data protection as a NED we have created a step-by-step data protection checklist.

1. Where is data protection on the board agenda? If it's not on there, why not?
2. Key boardroom questions to ask about data protection and the depth of the answers you should expect.
 - a. **Do we know what personal data we collect**, what we are doing with it, how long we keep it for and who we are sharing it with and why?
 - b. You should ask for a summary of the data audit/data map.
 - c. Where is our privacy policy? Is our privacy policy relevant and comprehensible by our volunteers, customers, staff and contractors.
 - d. Who has responsibility for data protection within the organisation? Do you have a **data protection officer (DPO)** or a data protection lead? Are they adequately resourced? Do they have relevant/appropriate experience? Are they able to report in directly to the board?
3. What data protection policies and procedures do we have in place? When were they last reviewed, updated and 'tested'?

a. **Data Protection Policy**

The 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 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 customers, employees/volunteers to understand and follow.

b. **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.



C. Privacy Policy

The privacy policy/notice is a key document as it lets your employees, customers, suppliers and contractors know that you take your privacy responsibilities seriously, it spells out how you use personal information and what they can do if they would like clarification as to your use of their information.

1. Who you are and what you do.
2. What information of theirs you hold and why.
3. How you obtained the information.
4. How you use the information.
5. How long you retain the information.
6. Whether you share the information, why and who with.
7. How information rights can be accessed.
8. Whether the data will be sent outside the EEA and safeguards in place.
9. Contact details for DPO (if required).
10. Right to Complain to JOIC.

D. Data/cyber security Policy

Keeping your IT systems safe and secure can be a complex task and does require time, resource and specialist knowledge. If you have personal data within your organisation's systems, you need to take appropriate technical measures to keep it safe and make sure no one can access it who doesn't have the authority to do so. The measures you put in place should fit the needs of your particular business.

E. Information Rights Policy

The DPJL gives individuals important personal information rights and places obligations on how both the public and private sectors process personal information. Organisations need to know how and who will be responsible for managing individual rights and the requests.

F. Breach policy and procedure

1. Does the organisation have a breach checklist?
2. How will the organisation respond to a personal data breach?

G. Working from home policy

Has the organisation considered;

- Security.
- Breach management and risk assessment.
- Training.



4. **New systems and processes – how we manage the implications of data protection.**

The DPJL requires you to put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights. This is 'data protection by design and **by default**'.

This means data protection is integrated into your processing activities and business practices, from the design stage right through the lifecycle.

Data protection by design is about considering data protection and privacy issues upfront in everything you do. It can help you ensure that you comply with the DPJL's fundamental principles and requirements, and forms part of the focus on accountability.

Consider the following areas;

- Governance – board & senior management activities and agendas.
- Data Protection by Design.
- Policies & procedures.
- Impact assessments.
- Internal & external communications.

5. What would be the impact of a data breach to the organisation?

- a. Worst case scenario.
- b. What is the breach action plan? Responsibilities etc.
- c. Breach reporting.
- d. Breach recording.

6. What technical and organisational measures are in place to manage personal data risk?

- a. Volunteer/staff training and refreshers.
- b. Processor agreements.
- c. Contractor agreements.
- d. Any data sharing agreements.
- e. Physical security.
- f. Accessibility to data/systems.
- g. Penetration testing.

7. Do you have staff buy in?

- a. Do they understand the organisations responsibilities/what they need to do to keep personal data safe and use it appropriately?
- b. Do the volunteers/staff receive appropriate training which is relevant to their role?
- c. Do the volunteers/staff know what to do and who to contact if something goes wrong?



8. How to stress test data protection as a NED.

- a. Ensure data protection is a standing item on the Board agenda
- b. Ensure data protection and cyber security forms part of your business risk assessment
- c. Evidence decisions on data protection matters – changes to systems or security, response to breaches, knowledge of complaints or request for personal information (subject access request)
- d. Receive periodic updates from your DPO/lead reports
- e. Ensure there is a clear breach escalation protocol that includes reporting of breaches to the Board
- f. Consider having a Board member with special responsibility for data protection.
- g. Think about data protection in business continuity planning e.g. remote working scenarios

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.

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