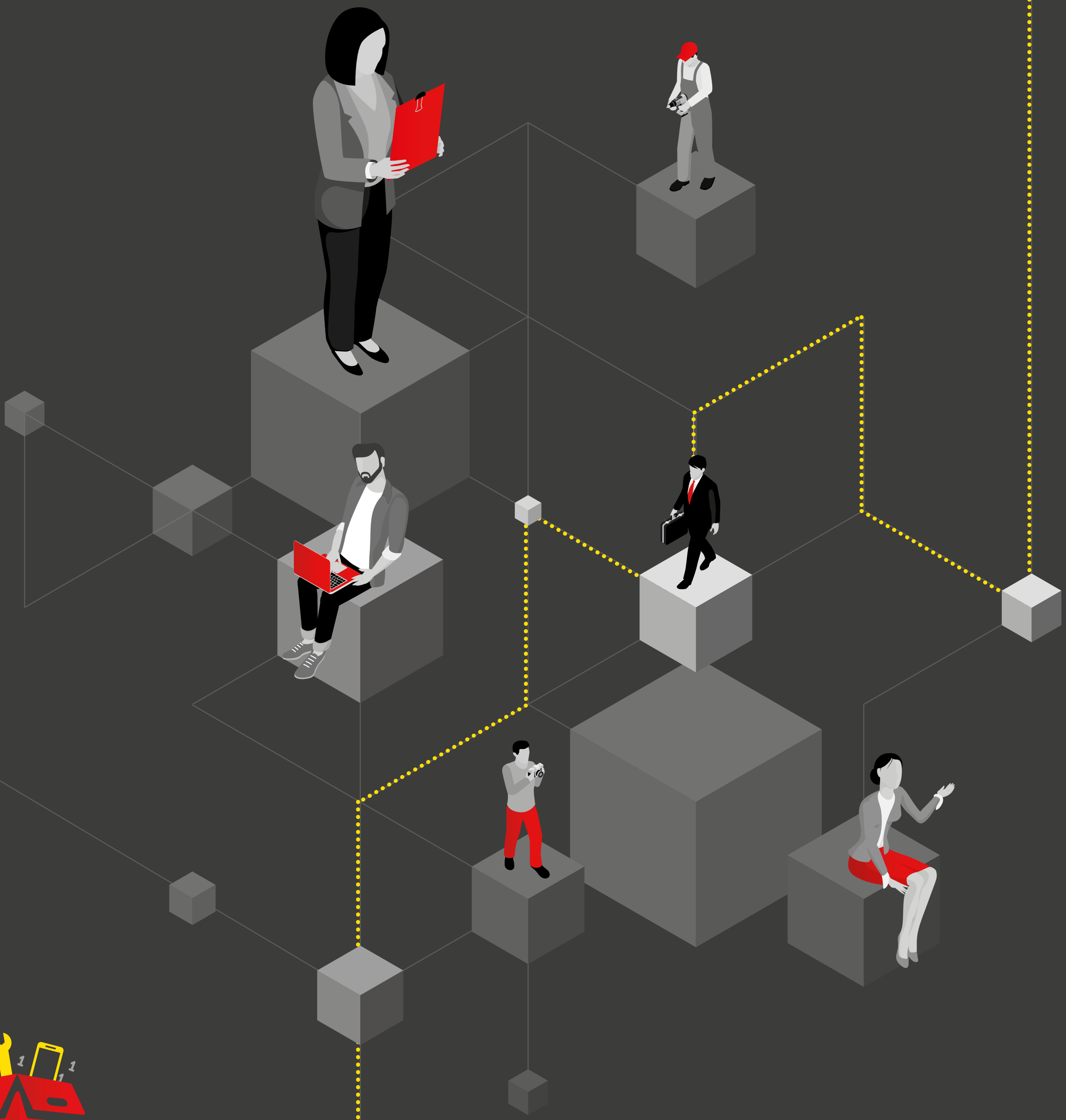
ORGANISATIONS

HOW TO STRESS TEST YOUR DATA PROTECTION TRAINING



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

Data Protection Training Checklist

To help ensure that the appropriate level of training is provided to meet your business and staff needs, we have created a data protection training checklist to help you assess what to look for in a training course and/or package. Please note that this checklist doesn't relate to Data Protection Officers as more role specific and specialist training is required.

Data protection training is not a one size fits all approach. Depending on the amount and types of personal information accessible in a person's role and the level of responsibility, training should be tailored to reflect the associated risk(s) of such. We expect that staff receive the relevant training which is refreshed on an appropriate frequency – so that knowledge is kept up-to-date, the frequency of training is to be assessed and noted internally. Consider the most suitable format for delivery, whether that be face-to-face, online, e-learning etc. Consider when this training will be delivered to new starters, i.e. during the induction process and how you are assessing competency levels of those taking the training. The level of training may need to be reconsidered during a change of role, if applicable.

The key areas of focus for training

We would suggest the following:

□ **1. What data protection laws are relevant to your business.**

a. Depending on your business structure, it may be that one or more data protection law apply to your organisation/charity/non-profit. Do you know which ones apply? i.e., Data Protection (Jersey) Law 2018 (DPJL), General Data Protection Regulation (GDPR) or similar. If established in Jersey, the DPJL is likely the primary legislation which will apply.

b. The training provider should tailor the training programme to the relevant law which actually applies to your business and the processing undertaken. If more than one applies, the trainers should highlight the differences and explain which law applies to which circumstances and if adhering to more than one, highlight the differences.

c. The **data protection principles** and how these reflected in your business. The trainer should focus extensively on the principles and their practical application and help to explain how these should be interpreted by your organisation.

□ **2. What is personal information and what types are classed as special category?**

a. What is personal information and what categories of personal information does your business process / use?
Any special category data?

b. If processing special category data, what additional measures should you have in place to ensure its security? E.g. limited staff members have access. What lawful basis is being relied upon that allows you to process the information (what are you processing and why?)

c. How does the business process the personal information collected? Are staff familiar and know where to find the privacy policy and is it accessible to data subjects (i.e. customers, members etc.)?

d. Does the organisation have a record of processing activities (ROPA) and is it kept up-to-date? Who has responsibility for this? The trainer should explain how the organisation creates and maintains the ROPA.

e. The training should consider applying the principles in **practice.** What do they look like within the organisation's processing activities.

□ 3. Key data protection terms and what they mean

What data protection terms do staff need to know? See our **Jargon Buster** for key terms under the DPJL.

□ 4. What isn't Data Protection

Trainer should explain what does data protection mean and who does it apply to? What does data protection cover and what does it not apply to? I.e. does not cover corporate / commercial data or animals.

□ 5. Breach Reporting

Training to cover what is a data breach and why it is important to know when this happens.

All staff should know how to identify a data protection breach, how and to whom it is to be reported to internally in a timely manner / as soon as possible. What is a data breach? Additional points to consider;

- What is an organisations breach procedure?
- Timescales – How long an organisation has to report a breach to JOIC, if it is considered reportable.
- Detail – What details need to be gathered about the incident so as to record internally, report to the JOIC and notify data subjects (if applicable to do so).
- Who is the point of contact for data protection in the organisation and who has responsibility for dealing with the breach (including any notification to JOIC). If they're not available, who is the secondary contact?
- Maintain an internal breach register / log where all data protection breaches should be logged.
- Lessons learned following a breach – could any measures be implemented to prevent recurrence? Do staff need further training / reminders?

□ 6. Best Practices / General Knowledge

Prevention is better than cure! In addition to being able to identify data breaches when they happen, it's equally, if not more important for staff to understand and be equipped to prevent them.

This will be dependent on people's positions within an organisation and business set-up. Some examples to think about;

- Phishing / Scam Emails – Do staff know how to recognise one and what to do if they receive one?
- Transporting Documents / Devices – Risks associated transporting documents and / or devices to and from different locations.
- Data Sharing – What information can be disclosed to 3rd party providers / business contacts? Are the necessary data processing / sharing agreements in place to do so? If unsure, speak to DPL or DPO. It is ok to challenge a request to share data with a 3rd party.
- Working from home / away from the office - Do you have any staff that work from home / away from the office? What measures are in place to ensure personal information remains protected.
- Data retention – do staff know how long data should be kept for and how to safely destroy it? Does the organisation have a data retention schedule or policy to support this?

What examples can you think of in your organisation?

□ 7. Individual Rights

This is a particularly important section which the trainer should explain carefully

a. Under the DPJL individuals have rights in respect of personal data held about them by others. Are staff aware of each of the rights and understand how to recognise requests that may come in?

b. Subject Access Requests can be received in many different ways, with this in mind it's important for all members of staff to know how to **recognise** one, and understand the internal procedure to follow upon receipt. Do they know who is authorised to deal with requests and what they can/cannot do?

c. What is the internal process for Subject Access Requests received – What are the timeframes and who is responsible for dealing with the request? See our **Subject Access Request Guidance** for further information.

□ 8. Data Protection Impact Assessments (DPIAs) / Risk Assessments

It may be appropriate to consider undertaking a Data Protection Impact Assessment (DPIA) or risk assessment in some, but not limited to, the following circumstances; when starting a new processing activity, implementing / using new technology or changing a process.

The trainer should teach about DPIAs / risk assessment and when to use.

a. Is the organisation undertaking or planning to undertake any processing that may result in a high risk to the rights and freedoms of data subjects and needs to undertake a DPIA? What does a DPIA look like? **(See our DPIA Template)**

b. If a DPIA is not required, has the organisation considered undertaking a more simplified risk assessment of the processing activity(ies) to assess the risk and any possible mitigation measures? These can be helpful to identify any potential risk(s) and what measures the organisation has taken or can take in order to mitigate such.

□ **9. Enforcement Action and Sanctions**

If things were to go wrong, what are the consequences?

Are staff aware of the action that could be taken upon the organisation should contravention of the law occur?

□ **10. The Jersey Office of the Information Commissioner**

Whilst interaction with our office will likely come from the data protection officer or other contact within an organisation, it's useful for all members of staff to know who we are, our role as a regulator and how we can support them. Our website has a range of resources for both individuals and organisations.

Finally, following implementing data protection training within your organisation, it's important to understand the effectiveness and whether it has been understood.

Measurement can be undertaken in many forms including, tests or completion of a case study. What is the best approach to suit your staff?

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.