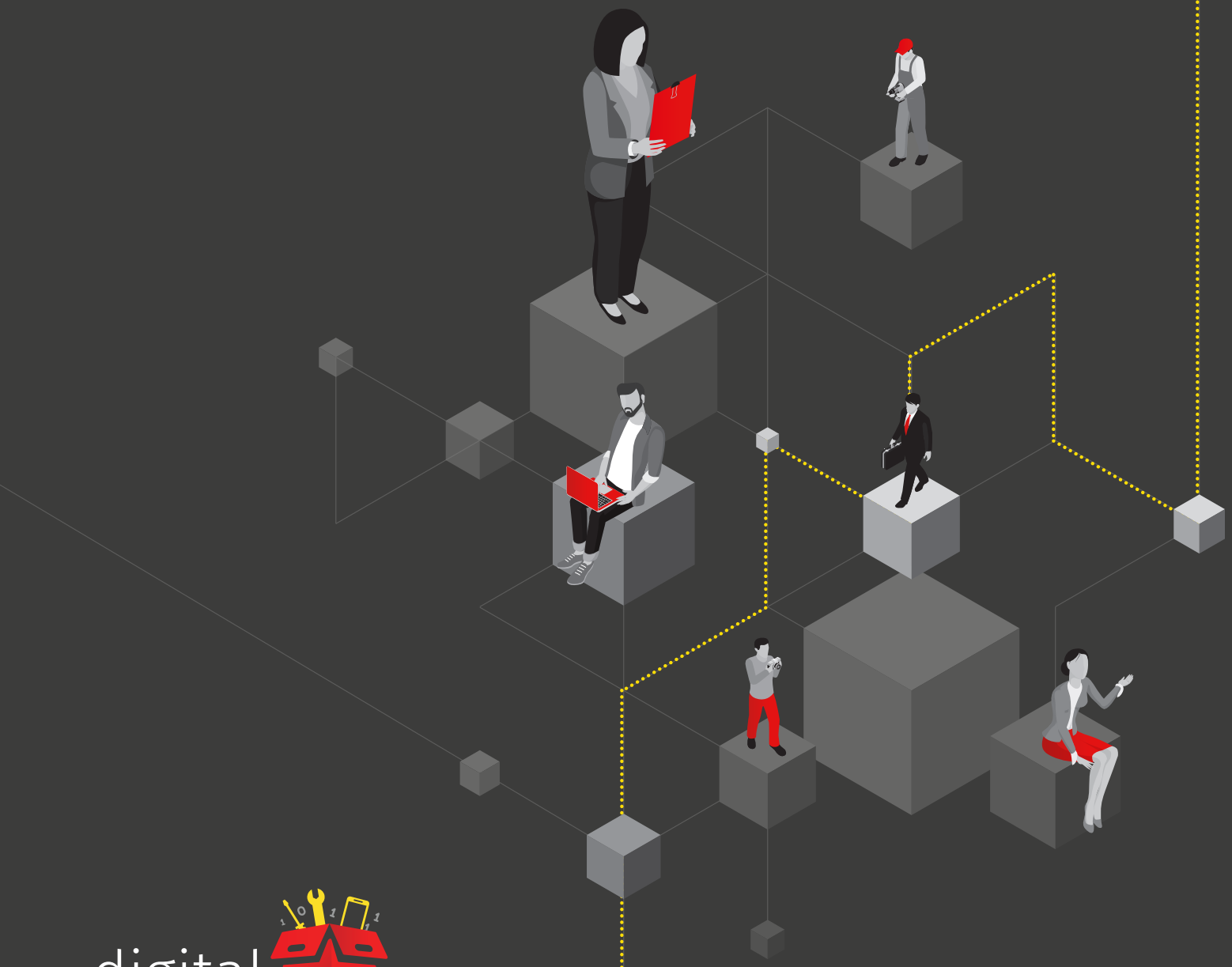
ORGANISATIONS

BIOMETRIC DATA
IN THE WORKPLACE



digital
TOOLKIT
Guidance for Organisations

JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

WWW.JERSEYOIC.ORG

Biometric Data Checklist

Biometric technologies offer the capability to improve the security of access to facilities and information systems. Nevertheless, they present greater risks to the rights and freedoms of individuals and because of this, additional requirements are placed on businesses.

Biometric technologies may allow the identification of individuals through fingerprint, iris scan, facial recognition or voice recognition. The Data Protection (Jersey) Law 2018 (the DPJL) requires additional safeguards when processing special category data (biometric information falls within this definition).

Accordingly, if you are considering implementing biometric technologies, you should take the following steps:

- Determine whether the use of biometric technology is absolutely necessary. If there are other less privacy-invasive means of achieving the same objective, use them instead. Ask yourself the following questions:

Would using ID badges fail to meet your needs?

☐ Yes ☐ No

Do your requirements go beyond just facilitating comfort and convenience?

☐ Yes ☐ No

Does your facility contain sensitive data?

☐ Yes ☐ No

If you answered 'No' to any of the three questions, do not use biometric technology for your purpose.

If you have answered 'Yes' to all three questions, proceed to the next step.

- Under the DPJL, where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons, a controller must carry out an assessment of the impact of the envisaged processing operations on the protection of personal data before the processing commences, known as a data protection impact assessment (**DPIA**). A DPIA must contain the following minimum requirements:
    - » A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
    - » An assessment of the necessity and proportionality of the processing operations in relation to the purposes;
    - » An assessment of the risks to the rights and freedoms of natural persons;
    - » The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the DPJL, taking into account the rights and legitimate interests of any person.

- After completing the DPIA, ensure that you have appropriately mitigated any risks identified and that you are able to demonstrate your compliance by putting appropriate technical and organisational measures in place;
- If your DPIA indicates that any processing would post a high risk to the rights and freedoms of individuals in the absence of measures taken by you to control the risk, you must consult the JOIC about the intended processing (see Art.17 of the DPJL);
- Ensure that you have a legal basis for collecting this biometric data. If you rely on the consent of individuals (including employees in an employment context), any consent you obtain from them must be explicit;
- In appropriate cases, consult with the trade union or other body representing the affected employees, prior to implementing the technology;
- Biometric systems involve the storage of a biometric template, such as a copy of a fingerprint or a facial recognition code. There are different options with respect to the storage and control of the template:
    - » The individual has complete control of the storage of the template (type 1);
    - » The individual has a secure password that is necessary to access the template (type 2);
    - » The controller has complete control of the storage of the template (type 3).

Type 1 provides that greatest level of protection for the individuals who data is stored, and you should use it wherever possible.

Type 2 is the next best option.

Type 3 should be a last resort, when no other option is possible.

- [ ] Ensure that you have documented all decisions regarding implementing biometric technologies, explaining your reasons. You may receive requests to justify your actions;
- [ ] Ensure that each step you take conforms with all requirements of the DPJL;
- [ ] Ensure that you are transparent with individuals about the way in which their data is being processed, what it's being used for and how they can exercise their rights;
- [ ] Ensure that your data protection officer/data protection lead is involved at each stage of the design, review and implementation process. Consult our office when the DPJL says you must and, in any event, if you require guidance or assistance.