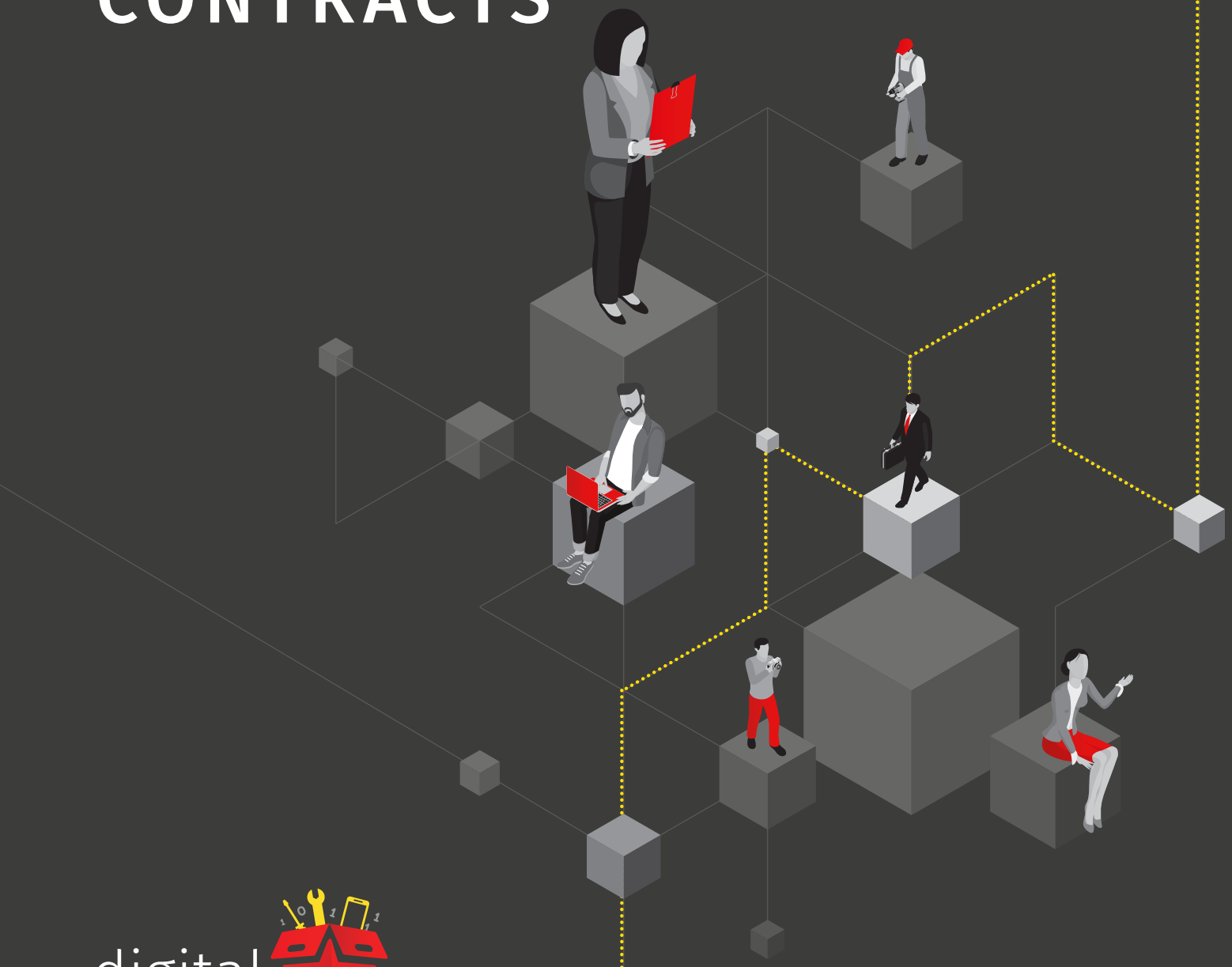
ORGANISATIONS

DATA CONTROLLER AND DATA PROCESSOR - **CONTRACTS**



digital **TOOLKIT**

Guidance for Organisations

JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

WWW.JERSEYOIC.ORG

Contracts at a Glance

Whenever a controller uses a processor, there must be a written contract (or another legal document) in place.

Whilst mandatory, having a written contract is important so that both parties understand their responsibilities and liabilities and so that there is written evidence of what arrangements are in place.

The Data Protection (Jersey) Law 2018 (DPJL) sets out what needs to be included in the contract.

The DPJL makes written contracts between controllers and processors a requirement, rather than just a way of demonstrating compliance with the integrity and confidentiality principle (appropriate security measures).

These contracts must include specific minimum terms. These terms are designed to ensure that processing carried out by a processor meets all the DPJL requirements, not just those related to keeping personal data secure.

When is a contract needed and why is it important?

Whenever a controller uses a processor to process personal data on their behalf, a written contract needs to be in place between the parties. Contracts between controllers and processors ensure they both understand their obligations, responsibilities and liabilities and that there is written evidence of what is expected of the parties. Contracts also help them comply with the DPJL, and assist controllers in demonstrating to individuals and regulators their compliance as required by the accountability principle.

A controller must only use processors that provide sufficient guarantees to implement appropriate technical and organisational measures to meet the requirements as stipulated in the DPJL and so as to ensure the protection of the rights of data subjects.

If a processor uses another organisation (i.e. a sub-processor) to assist in its processing of personal data for a controller, it must have a written contract in place with that sub-processor, have permission from the Controller (either specific or general written authorisation) and where the authorisation is general it must notify the controller of any intended changes so that the Controller has the opportunity to raise any objections.

Please remember that if the sub-processor fails in its obligations that the original processor remains fully liable to the controller for the performance of the sub-processor's obligations.

What responsibilities and liabilities do controllers have when using a processor?

Controllers must only use processors that can give sufficient guarantees they will implement appropriate technical and organisational measures to ensure their processing will meet DPJL requirements and protect data subjects' rights.

Controllers are primarily responsible for overall compliance with the DPJL, and for demonstrating that compliance. If this isn't achieved, they may be liable to pay damages in legal proceedings or be subject to fines or other penalties or corrective measures (including civil remedies sought by affected data subjects).

What responsibilities and liabilities do processors have in their own right?

In addition to its contractual obligations to the controller, a processor has some direct responsibilities under the DPJL. If a processor fails to meet its obligations, or acts outside or against the controller's instructions, it may be liable to pay damages in legal proceedings or be subject to fines or other penalties or corrective measures (including proceedings initiated by a controller if the processor fails to adhere to its contractual and/or legal obligations).

Extract from the DPJL Article 22 (3) & (4)

(3) A processor is liable to a data subject for any damage suffered as a result of processing that contravenes this Law.

(4) However, the processor is liable for the damage only where –

(a) it has not complied with the obligations placed on processors by this Law; or

(b) it acted outside of or contrary to the lawful instructions of the controller.

A processor may not engage a sub-processor's services without the controller's prior specific or general written authorisation. If authorisation is given, the processor must put in place a contract with the sub-processor. The terms of the contract that relate to Article 19(6) of the DPJL must offer an equivalent level of protection for the personal data as those in the contract between the controller and processor. Processors remain liable to the controller for the compliance of any sub-processors they engage.

Checklist

What to include in the contract:

The contract needs to set out details of the processing including:

- [ ] The subject matter of the processing;
- [ ] The duration of the processing;
- [ ] The nature and purpose of the processing (including dealing with any transfers);
- [ ] The type of personal data involved;
- [ ] The categories of data subject;
- [ ] The controller's obligations and rights.

The contract or other legal act must also include terms or clauses stating that:

- [ ] The processor must only act on the controller's documented instructions (including with regard to transfers to a third country or international organisation), unless required by law (in which case the processor must inform the controller of that legal requirement before processing, unless that law prohibits such information being given);

- [ ] The processor must ensure that people processing the data are subject to a duty of confidentiality;

- [ ] The processor must take appropriate measures to ensure the security of processing;

- [ ] (Where required) The processor must only engage a sub-processor with the controller's prior authorisation and under a written contract and advise the controller of any proposed change to the sub-processor so that the controller has the opportunity to object;

- [ ] The processor must take appropriate measures to help the controller respond to requests from individuals to exercise their rights (including notifying the controller if they receive a subject access request from an individual);

- [ ] Taking into account the nature of processing and the information available, the processor must assist the controller in meeting its DPJL obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;

- [ ] The processor must delete or return all personal data to the controller (if required by the controller) at the end of the contract, and the processor must also delete existing personal data unless they need to retain it for some other legal purpose;

- [ ] The processor must make available to the controller all information necessary to demonstrate compliance with the law including submitting to audits and inspections. The processor must also give the controller whatever information it needs to ensure they are both able to meet their respective obligations as set out at Article 19 of the DPJL.

Helpful extract from the DPJL

19 Appointment of processor

(1) Where processing is to be carried out on behalf of a controller, the controller must use only processors that provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Law and ensure the protection of the rights of the data subject.

(2) The processor must not engage another processor without prior specific or general written authorisation of the controller, and where the authorisation is general, the processor must inform the controller of any intended changes concerning the addition or replacement of other processors, so that the controller may object to the changes.

(3) Processing by a processor must be governed by a contract or other legal act under the relevant law, that –

(a) is binding on the processor with regard to the controller; and

(b) sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

(4) The contract or other legal act must, in particular, stipulate that the processor –

(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by the relevant law to which the processor is subject, in which case the processor must inform the controller of that legal requirement before processing, unless that law prohibits such information being given;

(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) takes all measures required by Article 21;

(d) respects the conditions referred to in paragraphs (2), (6) and (7) for engaging another processor;

(e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights set out in Part 6;

(f) assists the controller in ensuring compliance with the obligations under Articles 16, 20 and 21, taking into account the nature of processing and the information available to the processor;

(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless the relevant law requires storage of the personal data;

(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allows for and contributes to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

(5) *With respect to paragraph (4)(h), the processor must immediately inform the controller if, in its opinion, an instruction infringes this Law or other data protection provisions of the relevant law.*

(6) *Where the processor engages another processor the obligations set out in paragraph (4) must, in particular, provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Law and where that other processor fails to fulfil those obligations, the initial processor remains fully liable to the controller for the performance of that other processor's obligations.*

(7) *Adherence to a code or evidence of certification may provide evidence that an individual processor has complied with paragraphs (1) and (6).*

(8) *Without limiting the provisions of an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraph (4) may be based, in whole or in part, on standard contractual clauses as referred to in paragraph (9).*

(9) *The Authority may publish standard contractual clauses for the matters referred to in paragraphs (4) to (6).*

(10) *The contract or the other legal act referred to in this Article must be in writing.*

20 Notification of breach

(1) *In the case of a personal data breach, the controller must, without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach in writing to the Authority in the manner required by the Authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.*