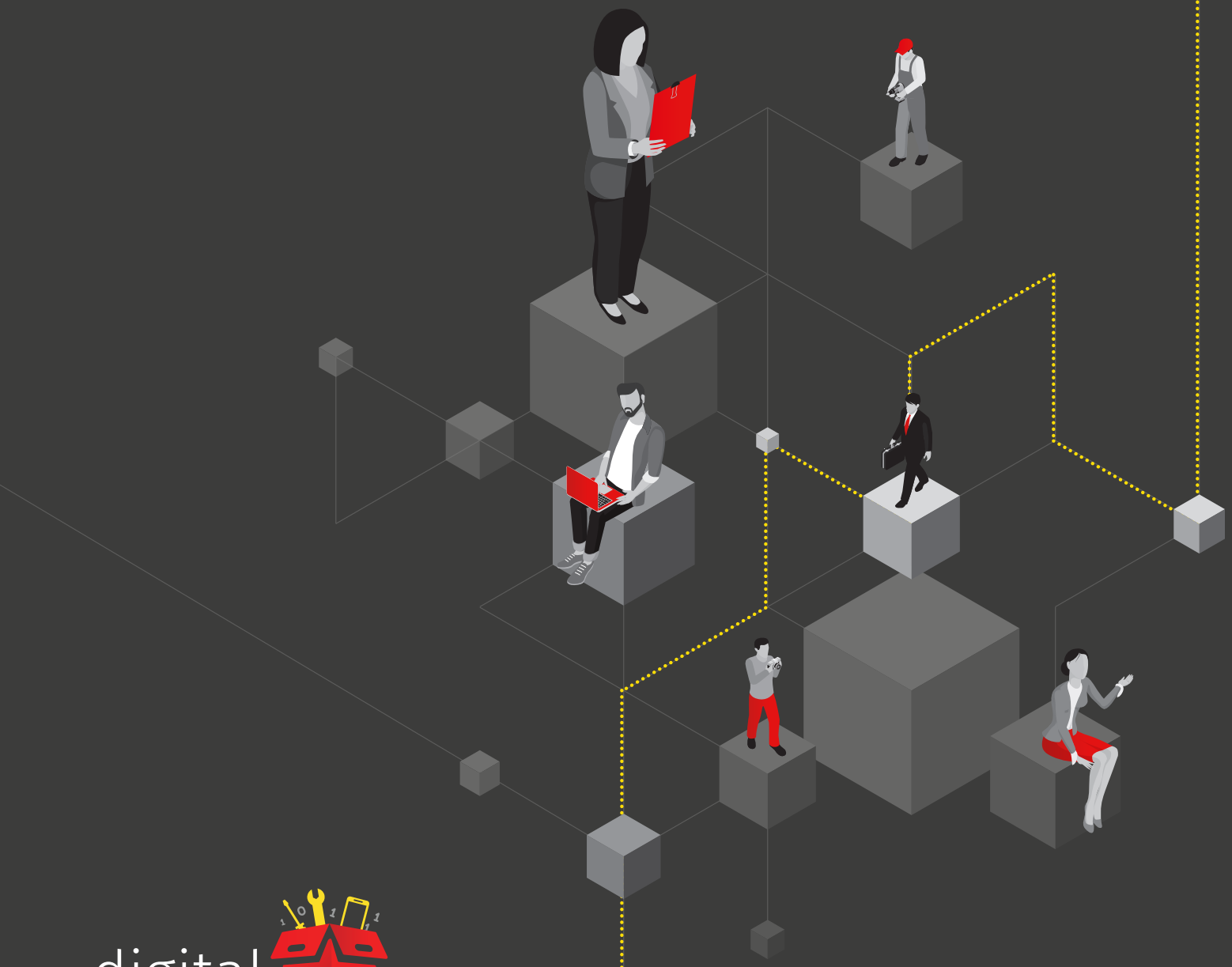
ORGANISATIONS

BREACH REPORTING



digital TOOLKIT

Guidance for Organisations

JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

WWW.JERSEYOIC.ORG

Introduction

1. The Data Protection (Jersey) Law 2018 (**DPJL**) is based around six principles of 'good information handling'. These principles give people (the data subjects) specific rights in relation to their personal information and place certain obligations on those organisations that are responsible for processing it.
2. This is part of a series of guidance to help organisations fully understand their obligations, as well as to promote good practice.
3. This guidance explains to organisations when and how to notify the Jersey Office of the Information Commissioner (the **JOIC**) about a personal data breach.
4. This guidance relates only to the DPJL.

Overview

- This guidance applies to data controllers, as defined under Art.1 of the DPJL;
- Data Controllers must notify the Commissioner that a personal data breach (a **breach**) has occurred without undue delay and, where feasible, not later than 72 hours after having become aware of it;
- A breach does NOT need to be notified to the Commissioner where it is unlikely to result in a risk to the rights and freedoms of natural persons in respect of their personal data;
- The JOIC provides a secure online form for all notifications;
- If there is a high risk that the breach is likely to result in a risk to the rights and freedoms of natural persons, the data controller must also notify those individuals:
    - » Without undue delay;
    - » In clear and plain language describing the nature of the breach; and
    - » Provide them with the name and contact details of the data controllers' **Data Protection Officer** (**DPO**), a description of the likely consequences of the breach and the measures taken or proposed to be taken by the controller to address the breach including, where appropriate, measures to mitigate its possible adverse effects.
- Data controllers must also keep a **log of any breaches**.

Relevant breaches

5. Under Art.20 (1) of the DPJL, data controllers have a specific obligation to notify the Commissioner - and in some cases affected individuals - about a breach, unless the breach is *'unlikely to result in a risk to the rights and freedoms of natural persons'*.
6. They are also required to keep a log of those breaches.
7. It is important to remember that the purpose of these provisions is to protect individuals' data and privacy. Therefore, it is important for organisations to consider the type of personal data they hold and whether any breach could adversely affect an individual - for example by causing financial loss, reputational damage or identity fraud.
8. If an organisation is responsible for delivering part of a service for a data controller but does not have a direct contractual relationship with an individual, it does not have to notify the Commissioner of a breach but it must immediately notify the data controller (who will have the contractual relationship with the individual) and it will be for the data controller to notify the Commissioner, as appropriate.

What is a breach?

9. A breach is defined in Art.1 of the DPJL as:

   '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 transmitted, stored or otherwise processed.'

10. In short, there will be a breach whenever any personal data (including any special category data) is accidentally lost, corrupted or disclosed, or if someone accesses it or passes it on without proper authorisation to do so.
11. A breach may be broadly defined as an incident which affected the availability, integrity or confidentiality of the personal data. This therefore includes a network intrusion by an unauthorised third-party and also a deliberate or accidental action by the service provider. For example, an employee causing the unintended deletion of personal data and where no appropriate back-up exists would constitute a breach. Whilst there is a threshold for seriousness in that breaches that are unlikely to result in a risk to the rights and freedoms of natural persons need not be reported, if there is any doubt, REPORT IT.

Breaches of encrypted information

12. Even if the personal data was encrypted to an appropriate standard, and the decryption key remains secure, data controllers must still notify us of the breach.

Notifying the Commissioner

13. Art.20 (1) of the DPJL states:

   '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.'

Within 72 hours of becoming aware

14. In other words, data controllers must tell us within 72 hours of becoming aware that a breach has occurred. As soon as they have enough information to confirm that there has been a breach and provide some basic facts, even if they can't yet provide full details. If a notification is not made to the Commissioner within 72 hours, the notification 'must be accompanied by reasons for the delay' (Art.20 (2) of the DPJL).
15. We do accept that in many cases it will not be feasible to provide us with full details within 72 hours. In such cases, Art.20 (4) of the DPJL states that:

   'Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.'

16. Accordingly, a data controller should still make the initial notification within 72 hours, essentially just to tell us that they have detected a breach and to provide us with the relevant contact details for the DPO. This should then be followed up with any of the outstanding information, as soon as the outstanding information is available.
17. We appreciate that data controllers may need to undertake an investigation to understand exactly what has happened and what needs to be done to mitigate the breach, and that in some cases this will take longer than 72 hours. However, data controllers must still notify us of the existence of the breach within 72 hours of having become aware of it, justifying and explaining why any further time is needed to investigate. We will expect data controllers to prioritise the investigation, to make adequate resources available to facilitate the investigation and to expedite matters as a matter of utmost urgency. Where, any details are missing from the initial notification, the required information may be provided in phases without undue further delay.

What information to include

18. Include as much as possible and follow up with missing information when available:
    - The name of the data controller;
    - The name and contact details of the DPO or other point of contact where more information can be obtained;
    - The date and time of the breach (or best estimate);
    - How the breach occurred;
    - The date and time of the controller becoming aware of the breach;
    - The nature and content of the personal data concerned;
    - If any special category data was breached;
    - Actions taken so far and/or planned to address the breach, including, where appropriate, measures to mitigate its possible adverse effects on the data subjects;
    - The number and category of data subjects concerned;
    - The likely consequences of the personal data breach and potential adverse effects on the data subjects;
    - The technical and organisational measures taken or proposed to be taken;
    - The number of data subjects notified;
    - Whether the breach affects data subjects in any jurisdiction other than Jersey;
    - Names of other data protection authorities;
    - Have police been notified;
    - Breach source i.e. data processor;
    - If these details cannot be provided a reasoned justification for the delay.

19. We provide a secure notification web form for data controllers to use to notify us of breaches. Additional documentation or information can be emailed separately to us at our breach notification email address: **breach@jerseyoic.org**

Useful reading

24 - Article 29 Working Party Guidelines on Personal Data Breach Notifications.

What happens next?

20. We will consider the information provided to assess whether the data controller is complying with its obligations under the DPJL including the duty to take appropriate technical and organisational measures to safeguard the personal data of the data subjects, the duty to notify us of a breach and the duty to notify the data subject of a Breach which is likely to result in a risk to their privacy.
21. Upon submission of an initial notification, a member of the JOIC team will respond accordingly at the first available opportunity to indicate what the next steps will be.

Notifying data subjects

22. Art.20 (6) of the DPJL states:

    'If the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller must communicate the Breach to the data subject -

    (a) Without undue delay; and

    (b) In clear and plain language describing the nature of the personal data breach; and

    (c) Giving the information and measures referred to in paragraph (3)(b) to (d)'
23. In other words, data controllers must also notify those individuals affected by the breach if such is likely to result in a high risk of the breach adversely affecting them.

If a breach is likely to represent a high risk to their fundamental rights and freedoms

24. Whether the breach is likely to result in a high risk is primarily a decision for the data controller, based on the circumstances of the case. The Commissioner considers that data controllers should consider the following factors:

    (a) The nature and content of the personal data;

    (b) Whether it includes special category data (as defined in the DPJL);

    (c) What harm could be caused to the individual – and in particular, whether there is a threat to the individual's physical safety or reputation, identity theft, fraud, financial loss, psychological distress or humiliation;

    (d) Who now has access to the data, to the extent this is known.
25. A data controller does not have to notify data subjects if the information was properly encrypted when the breach occurred or if the data controller has taken *'subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph (6) is no longer to materialise'* (Art.20 (70(b) of the DPJL).
26. Similarly, the data controller does not have to notify data subjects *'if it would involve disproportionate effort, in which case there must be a public communication or similar measure whereby the data subjects are informed in an equally effective manner'* (Art.20(7)(c) of the DPJL).

What to tell data subjects

27. In accordance with Art.20(6) of the DPJL any notification to data subjects must include the following information:
    - The name and contact details of the DPO or other contact point where more information can be obtained;
    - A summary of the likely consequences of the breach;
    - A description of the measures taken or proposed to be taken by the data controller to address the breach;
    - A description of the measures a data subject could take to mitigate any possible adverse effects of the breach.
28. In addition, we recommend that the notification to data subjects includes a helpline number or web address, if possible. The notification must be in clear and plain language.

When and how to notify data subjects

29. Data controllers must notify affected data subjects without undue delay – in other words, as soon as the data controller has sufficient information about the breach. However, if there are reasonable grounds to suspect that notifying data subjects may prejudice the investigation of the breach, you may seek authority from the Commissioner to delay that notification.

Keeping a log of personal data breaches

30. Art.20 (5) of the DPJL requires data controllers to keep a log of any breach:

    'The controller must document any personal data breaches, including the facts relating to the personal data breach, its effects and the remedial action taken, in such detail as will enable the Authority to verify its compliance with this Article.'

31. This means maintaining an inventory of data breaches. We have produced a template log to help you record the information you need.
32. We will inspect such logs if a data controller becomes subject to an audit pursuant to Schedule 1, Paragraph 7 of the Data Protection Authority (Jersey) Law 2018. We will use the logs and any other relevant information to check that data controllers are complying with their obligations under the DPJL.
33. As the Jersey Office of the Information Commissioner is transparent in its regulatory activities and respects the Freedom of Information (Jersey) Law 2011, we may receive requests for a data controller's logs and associated information. We will take the data controller's views into account when considering any request.

More information

34. Additional guidance is available on our guidance pages with more information on other aspects of the DPJL.
35. This guidance has been developed drawing on the Commissioner's experience. It will be reviewed and considered from time-to-time in line with new decisions by the Commissioner and/or the Jersey courts.
36. It is a guide to our general recommended approach, although each individual case will likely be different and will be decided on the particular circumstances of the case.
37. If you need any further information about this, or any other aspect of the DPJL, please contact us or see our website www.jerseyoic.org

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