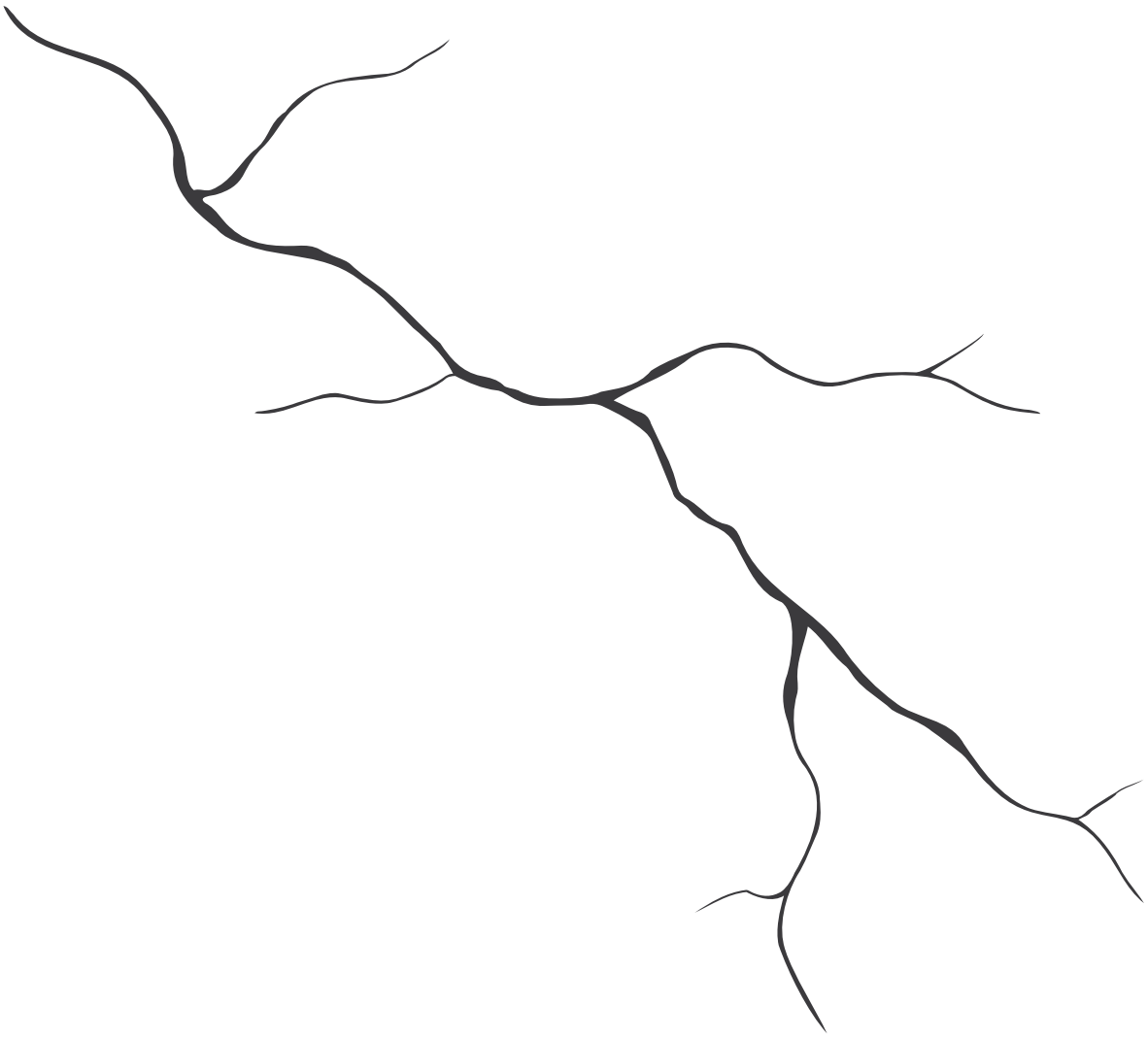
THE OFFICE OF THE
Data Protection
Authority

GUIDANCE:
Managing personal data breaches



2023 issue

Managing Personal Data Breaches

Overview
This guidance explains what a personal data breach is, what you should do if you experience one, and when and how to notify the Office of the Data Protection Authority (ODPA).

Who does this guidance apply to?
This guidance applies to controllers and processors who process personal data, in compliance with *The Data Protection (Bailiwick of Guernsey) Law, 2017* ('the Law').

It does not apply to data subjects[1] wishing to make a complaint about the way their personal data has been processed by a controller or processor, or in relation to their rights under the Law. If you are a data subject looking to make a complaint, please use this link: Make a Complaint.

What constitutes a personal data breach?
A personal data breach is defined by the Law as a breach of security leading to accidental or unlawful destruction, loss, or alteration of, or unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Examples of personal data breaches can include (but not limited to):

- Inappropriate access or disclosure of personal data
- Loss of personal data
- Data sent to the incorrect recipient (by e-mail or post etc.)
- System error resulting in the loss, alteration or access to personal data
- Cyber incidents

In the event of identifying a personal data breach, the Law stipulates a number of considerations and actions that you must take. These are explained in detail within the following sections of this document.

If the circumstances of the event in question do not fall within the scope of the above definition, the event is not a personal data breach and as such there are no specific requirements to take action under the Law.

Where an event is initially suspected to be a personal data breach but does not fall within the scope of the definition, you are advised to retain a written record of your assessment. It may also be appropriate to conduct a review of such an event to assess whether any improvements to technical or organisational measures could be put in place to mitigate any possible future similar 'near miss' event.

Does whether I am a Controller or Processor affect my response?
If you are a processor[2] and you become aware of a personal data breach, you must give the

[1] A **'data subject'** is the living person who is identified (or identifiable) by personal data. So you, your family members and friends etc. are referred to as 'data subjects' when your personal data is used by an organisation/entity.

[2] A **'processor'** is an entity that performs a task with personal data under instruction from a controller.
For example: if you outsource your payroll to an external company, that external company would be the processor for the set of personal data (name, bank details etc) relating to your staff being paid.

respective controller[3] notice of the breach as soon as practicable. Where this notice is given orally, you must follow up with written notice to the controller at the first opportunity.

If you are a controller and you become aware of a personal data breach, you are responsible for ensuring an appropriate response to the breach in compliance with the Law. A processor is not required to report personal data breaches to the Office of the Data Protection Authority (ODPA), however they must notify the respective controller as soon as practicable after becoming aware of the breach, as explained above.

Mitigating actions and post-breach review

When you become aware of a personal data breach, you must take appropriate action to mitigate any risk to all affected data subjects.

The action taken will very much be dependent on the specific circumstances of each breach, however, you must be able to demonstrate that you have considered such measures and implemented them where necessary. An example of such mitigating actions is retrieval/deletion of personal data sent to the incorrect recipient.

You should also conduct a review of the circumstances of the breach, identifying any shortfalls in your compliance with the Law that may have caused or contributed to the breach, and in turn implement any technical or organisational measures that may prevent similar breaches happening in future.

What information must I record?

The Law stipulates that a controller must keep a written record of every personal data breach that they become aware of, including the following information:

- The facts relating to the breach
- The effects of the breach
- The remedial action taken
- Any steps taken by the Controller to comply with Section 42 of the Law, including whether the Controller has given notice to the ODPA and a copy of that notice.

This information must be recorded and retained by the controller *regardless* of whether the personal data breach is reported to the ODPA or not. This record must be retained for a period of **6 years** from the day when the controller or processor first became aware of the breach.

Do I need to notify the ODPA?

A controller must give the ODPA written notification of all personal data breaches unless the personal data breach is unlikely to result in **any** risk to the 'significant interests' of the affected data subject(s).

Significant interests are defined as any of the following:

- Any rights or freedoms conferred by law on the individual
- The existence or extent of a duty imposed by law on the individual

[3] A '**controller**' is any entity who is responsible for the decisions made about why and how they use personal data about staff, customers, suppliers, or any other people. Note: an employee of a controller would be usually considered to be **part** of that controller.

- Any other interests of the individual that can reasonably be regarded as significant under the circumstances

Where is it assessed that the breach is unlikely to result in **any** risk to the significant interests of affected data subjects you must record your rationale as to why you believe that to be the case.

Written notification must be provided to the ODPA as soon as practicable, and in any event no later than 72 hours after the controller becomes aware of the breach, unless this is not practicable (rationale must be provided if notification is given later than 72 hours).

The Law specifies the information that must be provided in a notice to the ODPA. In order to make breach reporting easier for controllers there is a secure online reporting tool covering the requirements of the Law at: Report a Breach · ODPA.

With specific consideration to the 72 hour reporting period, if you have any issues reporting your breach using our online reporting tool, please contact the ODPA without delay by e-mail at breach@odpa.gg, or by telephone on 01481 742074.

Do I need to notify the affected data subject(s)?

Where there is likely to be a high risk to the significant interests of a data subject as a result of a personal data breach, the controller must give written notice to the data subject as soon as practicable after being made aware of the breach (unless any of the following points apply).

You are not required to give notice to a data subject in circumstances where:

- The personal data involved in the breach is unintelligible through use of technical and organisational measures such as encryption.
- The controller has taken subsequent sufficient mitigating measures which ensure that the risk is no longer likely to materialise.
- Notifying the data subject would require disproportionate effort.

The ODPA may also require that a controller notifies a data subject if it considers that the controller is obliged to do so under the Law.

A notice to data subjects must include:

- A description of the nature of the breach,
- The name and contact details of the data protection officer or other source where more information can be obtained,
- A description of the likely consequences of the breach, and
- A description of 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.

When assessing whether there is a high risk to the significant interests of data subjects, you must consider the nature, scope, context and purpose of the processing. You must consider any possible impact on the data subject resulting from the breach, as well as the likelihood of each possible impact occurring.

This is an assessment that you must make and be able to justify if questioned. As such, it is recommended that you record your rationale, especially if you conclude that a breach does not amount to a high risk to the significant interests of data subjects.

What happens when a breach is reported to the ODPA?

It is a common misconception that the main purpose of personal data breaches being reported to the ODPA is so that regulatory action can be taken against those that contravene the Law. Whilst regulatory action is a possibility, it is not the default response to reports of personal data breaches.

The main purpose of reporting personal data breaches is to ensure that such events are handled appropriately to mitigate further risk to data subjects and steps are taken to prevent future incidents.

When a personal data breach is reported to the ODPA we will complete an assessment of the circumstances and identify whether there is any further action that should be taken by the controller in response to the breach, including ensuring that appropriate consideration has been made as to whether any affected data subject should be notified.

In cases where it is proportionate to do so, taking account of factors such as the severity of the breach along with the controller's response to the breach, regulatory action may be considered.

Personal data breach reporting is also a vital conduit of information between the ODPA and the regulated community. This allows us to identify common trends, enabling us to raise awareness and focus our resources on issues that are of prevalence within our community.

When you report a personal data breach to us, we may contact you with further questions, and will let you know when we consider that the matter has been finalised or if regulatory action is to be taken.

Useful links to other resources:

- **Cyber security checklist**: https://www.odpa.gg/information-hub/guidance/cyber-security/
- **Bailiwick of Guernsey Police**: https://www.guernsey.police.uk/
- **Action Fraud** - the UK's national reporting centre for fraud and cybercrime https://www.actionfraud.police.uk
- UK Government's **National Cyber Security Centre** (NCSC) https://www.ncsc.gov.uk/

CONSIDERATIONS FOR A CONTROLLER TO MAKE UPON BECOMING AWARE OF A PERSONAL DATA BREACH: