THE OFFICE OF THE
Data Protection Authority

The Data Protection (Bailiwick of Guernsey) Law, 2017 ("the **Law**")

Notification of Personal Data Breaches

Introduction

The Law is based around seven principles of 'good information handling'. These principles give people (data subjects) specific rights in relation to their personal information and place certain obligations on those organisations that are responsible for processing it.

Breach reporting is a specific requirement under the Law and a copy of the Law can be found here.

This guidance explains to organisations when and how to notify the Office of the Data Protection Authority ("the ODPA") about a personal data breach.

Breach reports can be made via the secure breach reporting facility on our website :- https://odpc.gg/breach-reporting/.

Overview

- This guidance applies to controllers, as defined under section 111 of the Law .
- Controllers must provide the ODPA with written notice of a personal data breach (a breach) as soon as practicable and in any event no later than 72 hours after becoming aware of the breach. Where full details are not yet known, the initial notification may be followed up with further details as soon as practicable.
- All breaches that come to the attention of the controller after 25 May 2018 must be considered for reporting, regardless of when they occurred.

- Where a controller uses the services of a processor, the processor is required under section 42(1) of the Law to give the controller notice of a breach as soon as they become aware of it.

- Work is ongoing to prepare the reporting mechanism controllers will use to report a breach to the ODPA. Further information will be released once this is finalised. In the meantime, a form showing the information that will need to be reported is attached at the end of this guidance for your information.

- If it is likely that the breach will pose a high risk to the significant interests of a data subject, the controller must also notify those individuals:

    - As soon as practicable;
    - In clear and plain language;
    - Describing the nature of the breach; and
    - Providing them with the name and contact details of the controller's data protection officer (DPO) or other relevant contact, 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.

- Controllers must also keep a log of any breaches in accordance with section 42(6) of the Law. A template form for this purpose can be found at Appendix 1 but organisations can use their own if they wish.

Relevant breaches

Under section 42 of the Law, controllers have a specific obligation to notify the ODPA — about a breach, unless the breach is *'unlikely to result in a risk to the significant interests of a data subject*.

They are also required to keep a log of those breaches in accordance with section 42(6) of the Law.

Controllers are also required to disclose details of the breach to affected data subjects where there is a high risk to their significant interests (section 43)

It is important to remember that the purpose of these provisions is to protect individuals' personal data by ensuring appropriate steps are taken. 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 both at the time of the breach and in the future.

If an organisation is responsible for delivering part of a service for a controller but does not have a direct contractual relationship with the data subject, it does not have to notify the ODPA of a breach but it must immediately notify the relevant controller (who will have the contractual relationship with the data subject.) It will be for the controller to notify the ODPA and the data subject, as appropriate.

What is a breach?

A breach is defined in section 111(1) of the Law 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"*

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.

A breach may be broadly defined as an incident that 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 act by a service provider that disrupts the availability of personal data to those that need to use it. For example, the unintended deletion of personal data where no appropriate back-up exists would constitute a breach.

More information on what constitutes 'personal data' can be found here.

Notifying the ODPC

Section 42(2) of the Law states:

> *'Where a controller becomes aware of a personal data breach, the controller must give the Authority written notice of it as soon as practicable, and in any event, no later than 72 hours after becoming so aware,*

Controllers must therefore tell the ODPA no later than 72 hours of becoming aware that a breach has occurred. If a notification is not made to the ODPA within 72 hours, the notification must be accompanied by an explanation of the reasons for the delay (section 42(3)(e) of the Law).

It is accepted that in some cases it may not be feasible to provide full details within 72 hours. In such cases, section 42(4) of the Law states that:

> *'Where it is impracticable to give the Authority all of the required information at the same time as the notice is given, the controller may provide the information in phases as soon as practicable'*

Accordingly, a controller should still make the initial notification within 72 hours, to inform the ODPA that a breach has been detected and to provide the relevant details. This should then be followed up with any of the outstanding information and a follow up form is attached at the end of this document.

It may be the case that controllers 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, controllers must still notify the ODPA of the breach within 72 hours of having become aware of it and submit a follow-up notification as appropriate.

Breach reports can be made via the secure breach reporting facility on our website :- https://odpa.gg/breach-reporting/.

What information to include

The initial notification (within 72 hours) should ordinarily include the following summary information:

- The name of the controller
- The name and contact details of the DPO or other point of contact where more information can be obtained
- Whether it is a first or subsequent notification
- The date and time of the breach (or best estimate)
- The date and time of the controller becoming aware of the breach
- The nature and content of the personal data concerned
- Technical and organisational measures applied (or that will be applied) to the affected personal data
- The name of the organisation affected by the data breach (if different from the controller)

If possible, the initial notification should also include the more detailed information set out below. Otherwise, this should be included in any follow notifications until full details have been provided:

- A summary of the incident that caused the breach, including the physical location of the breach
- The number and category of data subjects concerned
- The number and category of personal data records 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 to mitigate those potential adverse effects
- The content of any notification provided to affected data subjects (where relevant)
- The means of communication used to notify the affected data subjects (where relevant)
- The number of data subjects notified (where relevant)
- Whether the breach affects data subjects in any jurisdiction other than the Bailiwick of Guernsey
- Details relating the notification with any other data protection authorities
- If these details cannot be included in any second notification, a reasoned justification for the further delay

What happens next

The information provided will be recorded by the ODPA and used to assess whether the controller is complying or has complied with its obligations under the Law, including the duty to take appropriate technical and organisational measures to safeguard the personal data of the data subjects, the duty to notify the ODPA of a breach and the duty to notify data subject of a breach which is likely to result in a risk to their significant interests.

Upon submission of an initial notification a controller will receive confirmation of receipt from the ODPA. An officer of the ODPA will contact the controller to indicate what the next steps will be.

Where a breach has affected or is likely to affect data subjects in jurisdictions outside of the Bailiwick of Guernsey, the ODPA may be required to communicate and cooperate with the relevant data protection authority in that jurisdiction / those jurisdictions in accordance with its statutory duties.

Notifying Data Subjects

Section 43 of the Law states:

> *"Where a controller becomes aware of a personal data breach that is likely to pose a high risk to the significant interests of a data subject, the controller must give the data subject written notice of the breach as soon as practicable.*

Controllers are therefore also required to notify those individuals affected by the breach if such is likely to result in any risk to their significant interests. Examples of such risks include financial loss, reputational damage, adverse impact of safety or wellbeing, and identity fraud. This list is not exhaustive and decisions should be informed by the nature, scope, context and purpose of the compromised personal data.

Whether the breach is likely to result in a risk to the significant interests of the data subject is primarily a decision for the controller and should be based on the circumstances of the case. The ODPA considers that 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 Law)
c. What harm could be caused to the individual both now and in the future – 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 may now have access to the data, to the extent this is known.

Section 43 of the Law states that a controller does not have to notify data subjects if the

> *"the controller has established and carried out appropriate technical and organisational measures to protect personal data, and those measures were applied to the personal data affected by the breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption" or if the controller has taken "subsequent measures which ensure that the high risk to the significant interests of data subjects referred to in subsection (1) is no longer likely to materialize"].*

Similarly, the controller does not have to notify data subjects *"if performing that duty would involve disproportionate effort",* in which case the controller must publish a notice (without making public any personal data) or take any other step equivalent to publication in order to inform the data subject in an equally effective manner" (section 43(5) of the Law).

What to tell data subjects

In accordance with section 43 of the Law any notice to data subjects must include the following information:

- 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
- A description of the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate, measures to mitigate the possible adverse effects.

In addition, it is recommended that the notification to data subjects includes a helpline number or web address, if possible.

The notification must be in clear and plain language. You may wish to consider publishing the notification in more than one language, depending on the nationalities of the data subjects affected.

It should be noted that whilst the decision whether or not to notify the affected data subject of the breach initially rests with the controller, the ODPA can require the controller to do so if, in its opinion, there exists a high risk to the significant interests of the data subject.

When to notify data subjects

Controllers must notify affected data subjects without undue delay – in other words, as soon as the controller has sufficient information about the breach.

Keeping a Log of Personal Data breaches

Section 42(6) of the Law requires controllers to keep a written record of any breach:

> *"In any case, a controller must keep a written record of each personal data breach of which the controller is aware, including –*
>
> *(a) The facts relating to the breach,*
>
> *(b) The effects of the breach,*
>
> *(c) The remedial action taken, and*
>
> *Any steps taken by the controller to comply with this section, including whether the controller gave a notice to the Authority under subsection (2), and if so, a copy of the notice.."*

The ODPA has created a template log to help you record the information you need – see Appendix 1.

The ODPA will inspect such logs if a controller becomes subject to an audit pursuant to Schedule 7, paragraph 9 of the Law. The logs and any other relevant information will be used to check that controllers are complying with their obligations under the Law.

More Information

If you need any further information about this, or any other aspect of the Law, please contact the ODPA or go to website www.odpa.gg.

Checklist

- ☐ We are clear about our breach reporting duties
- ☐ We have robust breach detection in place
- ☐ We have a breach response plan
- ☐ We have allocated responsibility for the handling, management, and oversight of breaches
- ☐ All staff have received appropriate training about prevention, detection and management of breaches
- ☐ We have a process to consider the impact of the breach on individuals
- ☐ We have a process to inform affected individuals where necessary
- ☐ We document all breaches regardless of the need to report

WRITTEN RECORD OF PERSONAL DATA BREACH

TEMPLATE FOR CONTROLLERS

Section 42 of the Data Protection (Bailiwick of Guernsey) Law, 2017 sets out the legal obligations of a controller in the event of a personal data breach. Section 42(6) states –

"*In any case, a controller must keep a written record of each personal data breach of which the controller is aware, including –*

(a) the facts relating to the breach,

(b) the effects of the breach,

(c) the remedial action taken, and

(d) any steps taken by the controller to comply with this section, including whether the controller gave a notice to the Authority under subsection (2), and if so, a copy of the notice."

This document allows affected controllers to record the required information in a uniform format to assist with internal record keeping obligations as well as requests for information from the Office of the Data Protection Authority (**ODPA**) that may follow. It does not constitute legal advice and each case should be reviewed in detail by the controller to assess the specific requirements.

Steps to take

- Immediately collect as much information as possible
- Ensure your DPO is informed and updated
- Report breach to ODPA
- Consider contacting interested parties (law enforcement, service provider)
- Implement containment measures
- Assess the harm
- Consider notification of data subjects
- Complete internal written record of the breach

APPENDIX 1

COMPANY NAME **HIGHLY CONFIDENTIAL**

FORM FOR RECORDING A PERSONAL DATA BREACH – INTERNAL USE		
YOUR NAME:		DEPT/DIVISION:
Today's Date:	Tel No:	E-MAIL ADDRESS:

Time & Date of Incident:	Time & Date Incident was discovered:
Who Was Notified:	Time of Notification:
Brief Summary of Incident: (include website URLs, suspect name(s), impacted system(s), other relevant data...)	
Number of data subjects affected:	
Location of affected data subjects:	
Type of personal data involved: Any special category data? If so, what?	

	Y	N
Did you witness the incident yourself?	☐	☐
Did others witness the incident? (if yes, specify below)	☐	☐

Summary of action taken since discovery:

Did you report this incident to: (Please circle all that apply)

Line Manager – IT Director – Internal Auditor – Data Protection Officer- ODPA – Law Enforcement – Guernsey Financial Services Commission

Initiated By:	Date:	Reviewed By:	Date: