information and privacy commission
new south wales

IPC Data Breach Policy

November 2016

Table of contents

Contents

Acknowledgement: The IPC acknowledges the use of guidance published by the Office of the Australian Information Commissioner and by the Office of the Information Commissioner Queensland in developing this policy.

Introduction

This policy provides guidance for responding to a breach of Information and Privacy Commission (IPC) held data.

This policy sets out the IPC procedures for managing a data breach, including the considerations around notifying persons whose privacy may be affected by the breach.

Effective breach management, including notification where warranted, assists the IPC in avoiding or reducing possible harm to both the affected individuals/organisations and the IPC, and may prevent future breaches.

Summary

The purpose of this policy is to provide guidance to IPC staff for responding to a breach of IPC held data.

This policy sets out the IPC procedures for managing a data breach, including:

- providing examples of situations considered to constitute a data breach
- the steps involved in responding to a data breach
- the considerations around notifying persons whose privacy may be affected by the breach.
- template correspondence for notifying persons whos privacy may be affected by the breach

1. Scope

This policy applies to all staff and contractors of the IPC. This includes temporary and casual staff, private contractors and consultants engaged by the IPC to perform the role of a public official.

This policy will apply from the date of effect.

This policy will be reviewed bi-ennially and as required as best practice and government directives change.

2. Purpose

The purpose of this policy is to provide guidance to IPC staff for responding to a breach of IPC held data.

This policy sets out the IPC procedures for managing a data breach, including the considerations around notifying persons whose privacy may be affected by the breach.

Effective breach management, including notification where warranted, assists the IPC in avoiding or reducing possible harm to both the affected individuals/organisations and the IPC, and may prevent future breaches.

3. Repsonsibility

The Director, Business Improvement, has overall responsibility for implementation of IPC corporate policies.

4. What is a data breach?

A data breach occurs when there is a failure that has caused or has the potential to cause unauthorised access to IPC data, such as:

- Accidental loss or theft of classified material data or equipment on which such data is stored (e.g. loss of paper record, laptop, iPad or USB stick)
- Unauthorised use, access to or modification of data or information systems (e.g. sharing of user login details (deliberately or accidentally) to gain unauthorised access or make unauthorised changes to data or information systems)
- Unauthorised disclosure of classified material information (e.g. email sent to an incorrect recipient or document posted to an incorrect address or addressee), or personal information posted onto the website without consent
- Compromised user account (e.g. accidental disclosure of user login details through phishing)
- Failed or successful attempts to gain unauthorised access to IPC information or information systems
- Equipment failure

- Malware infection
- Disruption to or denial of IT services

A data breach most commonly, but not exclusively, results in unauthorised access to, or the unauthorised collection, use, or disclosure of, personal information.

5. Responding to a data breach

The IPC privacy contact officer, the Director Business Improvement, or CEO nominee must be informed of any data breach to ensure the application of this policy and advice to the CEO/Information Commissioner to assist in responding to enquiries made by the public, and managing any complaints that may be received as a result of the breach.

There are four key steps required in responding to a data breach:

1. Contain the breach.
2. Evaluate the associated risks.
3. Consider notifying affected individuals.
4. Prevent a repeat.

Each step is set out in further detail below. The first three steps should be carried out concurrently where possible. The last step provides recommendations for longer-term solutions and prevention strategies.

The Department of Justice supports the IPC in the supply and maintenance of its IT systems. The Director, Business Improvement or CEO nominee will coordinate with the Department of Justice to address and respond to identified data breaches related to its IT systems.

5.1 Step one: Contain the breach

Containing the breach is prioritized by the IPC. All necessary steps possible must be taken to contain the breach and minimise any resulting damage. For example, recover the personal information, shut down the system that has been breached, suspend the activity that lead to the breach, revoke or change access codes or passwords.

If a third party is in possession of the data and declines to return it, it may be necessary for the IPC to seek legal or other advice on what action can be taken to recover the data. When recovering data, the IPC will make sure that copies have not been made by a third party or, if they have, that all copies are recovered.

5.2 Step two: Evaluate the associated risks

To determine what other steps are needed an assessment of the type of data involved in the breach and the risks associated with the breach will be undertaken. Some types of data are more likely to cause harm if it is compromised. For example, personal information, health information, and security classified

information, will be more significant than names and email addresses on a newsletter subscription list. A combination of data will typically create a greater potential for harm than a single piece of data (for example, an address, date of birth and bank account details, if combined, could be used for identity theft).

Factors to consider include:

- **Who is affected by the breach?** The IPC assessment will include reviewing whether individuals and organisations have been affected by the breach, how many individuals and organisations have been affected and whether any of the individuals have personal circumstances which may put them at particular risk of harm.

- **What was the cause of the breach?** The IPC assessment will include reviewing whether the breach occurred as part of a targeted attack or through inadvertent oversight. Was it a one-off incident or does it expose a more systemic vulnerability? What steps have been taken to contain the breach? Has the data been recovered? Is the data encrypted or otherwise not readily accessible?

- **What is the foreseeable harm to the affected individuals/organisations?** The IPC assessment will include reviewing what possible use there is for the data. For example, could it be used for identity theft, threats to physical safety, financial loss, or damage to reputation? Who is in receipt of the data? What is the risk of further access, use or disclosure, including via media or online?

5.3 Step three: Consider notifying affected individuals/organisations

The IPC recognises that notification to individuals/organisations affected by a data breach can assist in mitigating any damage for those affected individuals/organisations and reflect positively on the IPC's reputation. Notification demonstrates a commitment to open and transparent governance, consistent with the IPC's approach. However reflective of established guidance the IPC adopts the approach that if the data breach creates a real risk of serious harm to the individual, the affected individuals should be notified.

In general, if a data breach creates a risk of harm to an individual/organisation, the affected individual/organisation should be notified. Prompt notification in these cases can help to avoid or lessen the damage by enabling the individual/organisation to take steps to protect themselves.

There are occasions where notification can be counter-productive. For example, information collected may be less sensitive and notifying individuals about a privacy breach which is unlikely to result in an adverse outcome for the individual may cause unnecessary anxiety and de-sensitise individuals to a significant privacy breach.

Factors the IPC will consider when deciding whether notification is appropriate include:

- What is the risk of harm to the individual/organisation?
- What steps has the IPC taken to date to avoid or remedy any actual or potential harm?
- What is the ability of the individual/organisation to take further steps to avoid or remedy harm?

- Even if the individual/organisation would not be able to take steps to rectify the situation, is the information that has been compromised sensitive, or likely to cause humiliation or embarrassment for the individual/organisation?
- Are there any applicable legislative provisions or contractual obligations that require the IPC to notify affected individuals?

The logistics of notifying affected individuals/organisations will depend in large part on the type and scale of the breach, as well as immediately practical issues such as having contact details for the affected individuals/organisations. Considerations include the following.

5.3.1 When to notify

In general, individuals/organisations affected by the breach should be notified as soon as practicable. Circumstances where it may be appropriate to delay notification include where notification would compromise an investigation into the cause of the breach or reveal a software vulnerability.

5.3.2 How to notify

Affected individuals/organisations should be notified directly - by telephone, letter, email or in person. Indirect notification – such as information posted on the IPC's website, a public notice in a newspaper, or a media release – should generally only occur where the contact information of affected individuals/organisations are unknown, or where direct notification is prohibitively expensive or could cause further harm (for example, by alerting a person who stole the laptop as to the value of the information contained).

5.3.3 What to say

The notification advice will be tailored to the circumstances of the particular breach.
Content of a notification could include:

- information about the breach, including when it happened
- a description of what data has been disclosed
- assurances (as appropriate) about what data has not been disclosed
- what the agency is doing to control or reduce the harm
- what steps the person/organisation can take to further protect themselves and what the IPC will do to assist people with this
- contact details for the IPC for questions or requests for information
- the right to lodge a privacy complaint with the Privacy Commissioner

The template at Appendix A will form the basis of this action.

5.4 Step four: Prevent a repeat

The IPC will further investigate the circumstances of the breach to determine all relevant causes and consider what short or long-term measures could be taken to prevent any reoccurrence.

Preventative actions could include a:

- security audit of both physical and technical security controls
- review of policies and procedures
- review of employee training practices; or
- review of contractual obligations with contracted service providers.

The template at Appendix B will be used for reporting on the investigation of the breach and authorising actions in response.

5.4.1 Notifying the NSW Privacy Commissioner

As a matter of good practice, the CEO will notify the NSW Privacy Commissioner of a data breach where required and when the circumstances indicate that it is appropriate to do so. The potential benefits of notifying the NSW Privacy Commissioner of a data breach may include the following:

- A decision by the IPC to notify on its own initiative is likely to be viewed by the public as a positive action. It demonstrates to the public that the IPC views the protection of personal information as an important and serious matter, and may therefore enhance public confidence in the IPC.

- The NSW Privacy Commissioner or delegate may be assisted in responding to enquiries made by the public and managing any complaints that may be received as a result of the breach. If the IPC provides the Privacy Commissioner or delegate with details of the matter and any action taken to address it, and prevents future occurrences, then, based on that information, any complaints received may be able to be dealt with more quickly.

Notification should contain similar content to that provided to individuals/organisations. The personal information about the affected individuals is not required. It may be appropriate to include:

- a description of the breach
- the type of personal information involved in the breach
- what response the IPC has made to the breach
- what assistance has been offered to affected individuals
- the name and contact details of the appropriate contact person, and
- whether the breach has been notified to other external contact(s).

Appendix A

TEMPLATE CORRESPONDENCE

Dear [**name**]

I am writing to you with important information about a recent data breach involving your personal information / information about your organisation. The Information and Privacy Commission became aware of this breach on [**date**].

The breach occurred on or about [**date**] and occurred as follows:

(Describe the event, including, as applicable, the following):

- A brief description of what happened.
- Description of the data that was inappropriately accessed, collected, used or disclosed.
- Risk(s) to the individual/organisation caused by the breach.
- Steps the individual/organisation should take to protect themselves from potential harm from the breach.
- A brief description of what the IPC is doing to investigate the breach, control or mitigate harm to individuals/organisations and to protect against further breaches.

Please call me with any questions or concerns you may have about the data breach.

We have established a section on our IPC website [**insert link**] with updated information and links to resources that offer information about this data breach.

We take our role in safeguarding your data and using it in an appropriate manner very seriously. Please be assured that we are doing everything we can to rectify the situation.

Please note that under the [PPIP Act / HRIP Act / GIPA Act] you are entitled to register a complaint with the NSW Privacy Commissioner or NSW Information Commissioner/CEO with regard to this breach. Complaints may be forwarded to the following:

[insert IPC details]

Should you have any questions regarding this notice or if you would like more information, please do not hesitate to contact me.

Yours sincerely,

[**Insert applicable name and contact information]**

Appendix B: TEMPLATE REPORT AND ACTION

Description of data breach	Action Taken
When - What - How –	Notification – Containment -
Description of risks	**Action Proposed**
Risk - Harm - Affecting –	
Description of causes	**Action Proposed**
How - Why -	Change – Train – Remind – Review – Stop – Media – Remedy – Etc –
Notification to the NSW Privacy Commissioner	

Director Business Improvement or CEO nominee		**Date:**	
CEO / Information Commissioner Approved / Not Approved / Noted		**Date:**	

6. Document information

Identifier/Title:	IPC Data Breach Policy
Business Unit:	Executive
Author:	Director Investigation and Reporting
Owner:	Director Business Improvement
Approver:	Chief Executive Officer
Date of Effect:	October 2016
Next Review Date:	October 2018
EDRMS File Reference:	D16/099948/DJ
Key Words:	Breach, notification, personal information, containment

7. Document history

Version	Date	Reason for Amendment
1.0	October 2016	Draft for internal consultation
1.1	November 2016	Revised draft to incorporate CEO/IC feedback
1.2	4 November 2016	Approved by CEO