Xeppo

Data Breach Notification Guide

Policies and Procedures

Introduction

This data breach policy is to be implemented in the event that Xeppo experiences a data breach.

A data breach occurs when personal information is lost or subjected to unauthorized access, modification, use, disclosure or other misuse. Data breaches can be caused or exacerbated by a variety of factors, affect different types of personal information and give rise to a range of actual or potential harms to individuals, agencies and organisations.

This plan is intended to enable Xeppo to contain, assess and respond to data breaches in a timely fashion and to help mitigate potential harm to affected individuals.

Responsibilities

Employees are responsible for:

- Adhering to the Policy.

Head of Product Development is responsible for:

- Containing and evaluating data breaches;
- Notifying, where appropriate, affected individuals;
- Conducting a review of the breach and report outcomes;
- Reporting all data breaches to the Xeppo Board.

Xeppo Board is responsible for:

- Advising AOIC of significant data breaches;
- Ensure legal implications have been addressed.

APPLICATION

STEP 1: Contain the breach and do a preliminary assessment

All employees are required to notify the Head of Product Development as soon as a data breach is suspected. The Head of Product Development will then:

(a) Review and contain the breach if confirmed

(b) Initiate a preliminary assessment

(c) Consider who needs to be notified immediately eg affected clients, businesses and Xeppo Board and keep appropriate parties informed

STEP 2: Evaluate the risks associated with the breach

The Head of Product Development in consultation with the Xeppo Development Team will consider the following factors in assessing the risks of the breach. Appropriate record keeping of all considerations and decisions are to be documented by the Head of Product Development.

(a) The type of personal information involved

1. Does the type of personal information that has been compromised create a greater risk of harm?
2. Who is affected by the breach?

(b) The context of the affected information and the breach

1. What is the context of the personal information involved?
2. What parties have gained unauthorised access to the affected information?
3. Have there been other breaches that could have a cumulative effect?
4. How could the personal information be used?

(c) The cause and extent of the breach

1. Is there a risk of ongoing breaches or further exposure of the information?
2. Is there evidence of theft?
3. Is the personal information adequately encrypted, anonymised or otherwise not easily accessible?
4. What was the source of the breach?
5. Has the personal information been recovered?
6. What steps have already been taken to mitigate the harm?
7. Is this a systemic problem or an isolated incident?
8. How many individuals are affected by the breach?

(d) The risk of serious harm to the affected individuals

1. Who is the recipient of the information?
2. What harm to individuals could result from the breach?

   Examples include:

   - identity theft
   - financial loss
   - threat to physical safety
   - threat to emotional wellbeing
   - loss of business or employment opportunities
   - humiliation, damage to reputation or relationships, or
   - workplace or social bullying or marginalisation.

(e) The risk of other harms.

Examples include:

- the loss of public trust in Xeppo
- reputational damage
- loss of assets (e.g., stolen computers or storage devices)
- financial exposure (e.g., if bank account details are compromised)
- regulatory penalties (e.g., for breaches of the Privacy Act)
- extortion

- legal liability, and
- breach of secrecy provisions in applicable legislation.

STEP 3: Notification

The Head of Product Development will notify the Xeppo Board of any data breach once confirmed. Action may be taken by the Head of Product Development including notification, prior to notifying the board if the breach is serious/significant. The Xeppo Board in conjunction with the Head of Product Development will:

(a) Decide whether to notify affected individuals

Consideration of the following factors will assist if notification is required (do you want more y/n ie item 1 if yes then is there a need to quantify or up to Rohan/Board to decide:

- Are multiple individuals affected by the breach or suspected breach?
- What is the risk of serious harm to the individual?
- What is the ability of the individual to avoid or mitigate possible harm if notified of a breach in addition to steps taken by Xeppo. For example, would an individual be able to have a new bank account number issued.
- If the individual would not be able to take steps to fix the situation, is the information that has been compromised sensitive, or likely to cause humiliation or embarrassment for the individual?
- What are the legal and contractual obligations to notify, and what are the consequences of notification?
- Does the breach or suspected breach indicate a systemic problem?
- Could there be media attention as a result of the breach?

(b) Notification process

At the conclusion of the preliminary and risk evaluation assessments a determination by the Xeppo Board whether to notify individuals/practices is to be made.

If the breach is serious as determined by the Head of Product Development, notification should happen immediately, before having all the relevant facts and Board approval.

1. When to notify?

   Individuals/companies? affected by the breach should be notified as soon as reasonably possible.

2. How to notify?

   Affected individuals should receive notification by phone, letter, email or in person.

3. Who should notify?

   The Head of Product Development is responsible for notifying affected individuals.

4. Who should be notified?

   Individual(s)/companies affected by the breach. However, in some cases it may be appropriate to notify the individual's guardian or authorised representative on their behalf.

(c) What should be included in the notification?

1. Incident Description ie type of personal information involved
2. Response to the breach
3. Assistance offered to affected individuals
4. Other information sources to assist individuals protecting themselves
5. Agency/Organisation contact details
6. Whether breach notified to regulator or other external contacts
7. Legal implications
8. How individuals can lodge a complaint with the agency or organization
9. How individuals can lodge a complaint with the OAIC

(d) Who else should be notified?

1. Lawyer
2. OAIC
3. Police
4. Insurers
5. Practices

6. Credit card companies, financial institutions
7. Professional or other regulatory bodies
8. Agencies that have a direct relationship with the information lost/stolen ie ATO for TFN, Medicare Australia for Medicare numbers

STEP 4: Prevent future breaches

The Head of Product Development will conduct a review and report to the Xeppo Team and Board the outcomes and subsequent recommendations. Outcomes may include:

(a) Development a prevention plan

A prevention plan should suggest actions that are proportionate to the significance of the breach and whether it was a systemic breach or an isolated event.

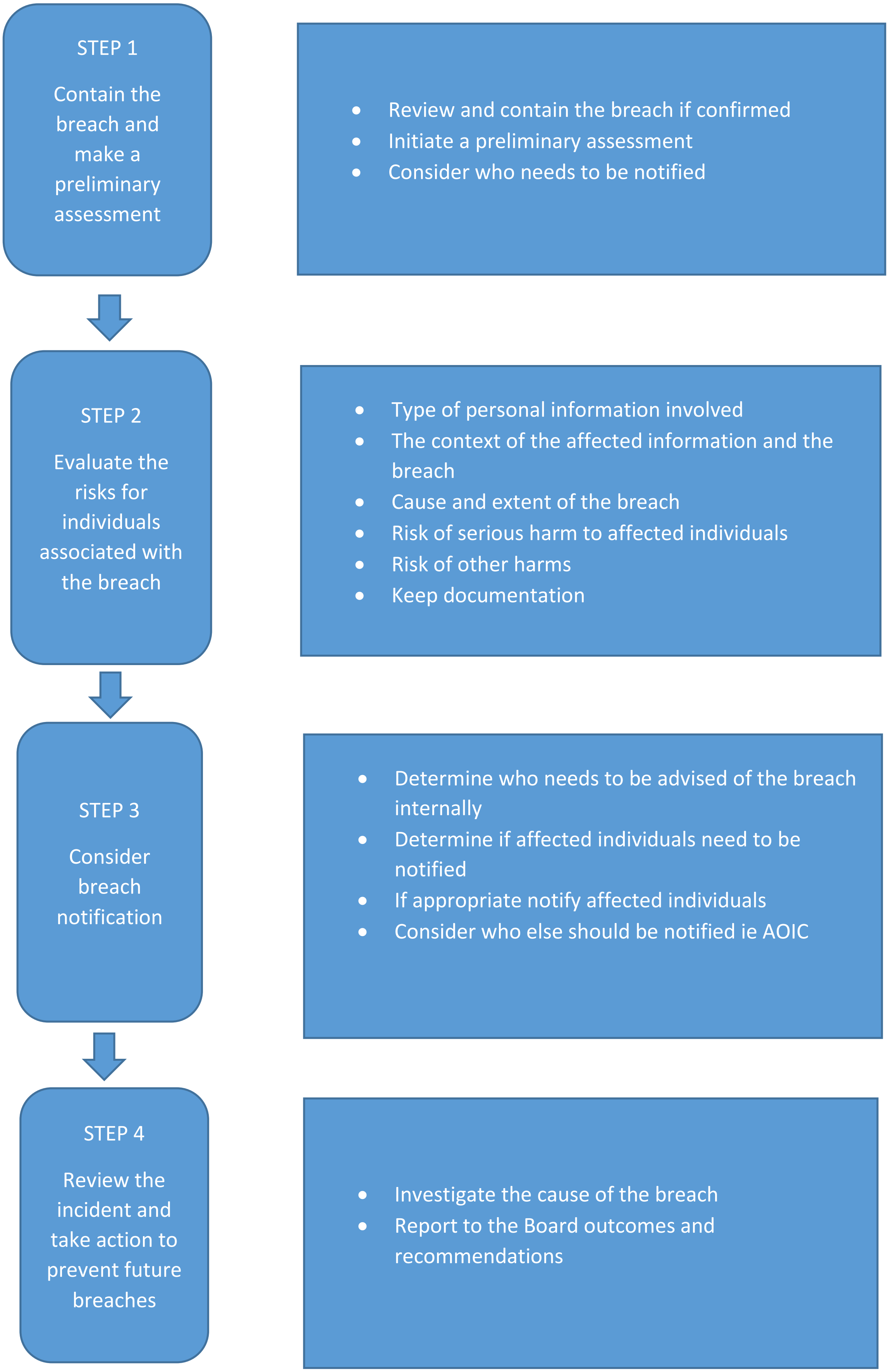
This plan may include:

- a security audit of both physical and technical security
- a review of policies and procedures and any changes to reflect the lessons learned from the investigation, and regular reviews after that (for example, security, record retention and collection policies)
- a review of employee selection and training practices, and
- a review of service delivery partners (for example, offsite data storage providers).
- a requirement for an audit at the end of the process to ensure that the prevention plan has been fully implemented.

(b) Development a breach response plan

(c) Establish a breach response team

(d) Enhance internal communication and training



STEP 1

Contain the breach and make a preliminary assessment

- Review and contain the breach if confirmed
- Initiate a preliminary assessment
- Consider who needs to be notified

STEP 2

Evaluate the risks for individuals associated with the breach

- Type of personal information involved
- The context of the affected information and the breach
- Cause and extent of the breach
- Risk of serious harm to affected individuals
- Risk of other harms
- Keep documentation

STEP 3

Consider breach notification

- Determine who needs to be advised of the breach internally
- Determine if affected individuals need to be notified
- If appropriate notify affected individuals
- Consider who else should be notified ie AOIC

STEP 4

Review the incident and take action to prevent future breaches

- Investigate the cause of the breach
- Report to the Board outcomes and recommendations

Reporting a data breach to the Office of the Australian Information Commissioner

Agencies and organisations are strongly encouraged to notify the OAIC of a data breach where the circumstances indicate that it is appropriate to do so, as set out in Step 3(d). The potential benefits of notifying the OAIC of a data breach may include the following:

- An agency or organisation's decision to notify the OAIC on its own initiative is likely to be viewed by the public as a positive action. It demonstrates to clients and the public that the agency or organisation views the protection of personal information as an important and serious matter, and may therefore enhance client/public confidence in the agency or organisation.

- It can assist the OAIC in responding to inquiries made by the public and managing any complaints that may be received as a result of the breach. If the agency or organisation provides the OAIC 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. In those circumstances, consideration will need to be given to whether an individual complainant can demonstrate that they have suffered loss or damage, and whether some additional resolution is required. Alternatively, the OAIC may consider that the steps taken have adequately dealt with the matter.

Note: Reporting a breach does not preclude the OAIC from receiving complaints and conducting an investigation of the incident (whether in response to a complaint or on the Commissioner's initiative).

If the agency or organisation decides to report a data breach to the OAIC, the following provides an indication of what the OAIC can and cannot do:

What the OAIC can do

- Provide general information about obligations under the Privacy Act, factors to consider in responding to a data breach, and steps to take to prevent similar future incidents.

- Respond to community enquiries about the breach and explain possible steps that individuals can take to protect their personal information.

What the OAIC cannot do

- Provide detailed advice about how to respond to a breach, or approve a particular proposed course of action. Agencies and organisations will need to seek their own legal or other specialist advice.

- Agree not to investigate (either using the Commissioner’s power to investigate on their own initiative, or if a complaint is made to the OAIC) if the OAIC is notified of a breach.

When the OAIC receives a complaint about an alleged breach of the Act, in most cases, the OAIC must investigate. As set out above, the OAIC may also investigate an act or practice in the absence of a complaint on the Commissioner’s initiative. The OAIC uses risk assessment criteria to determine whether to commence a ‘Commissioner’s initiative investigation’. Those criteria include:

- whether a large number of people have been, or are likely to be affected, and the consequences for those individuals

- the sensitivity of the personal information involved

- the progress of an agency or organisation’s own investigation into the matter

- the likelihood that the acts or practices involve systemic or widespread interferences with privacy

- what actions have been taken to minimise the harm to individuals arising from the breach, such as notifying them and/or offering to re-secure their information, and

- whether another body, such as the police, is investigating.

These factors are similar to those included in the risk assessment criteria for responding to a data breach.

What to put in a notification to the OAIC

Any notice provided to the OAIC should contain similar content to that provided to individuals (see page 25). It should not include personal information about the affected individuals. It may be appropriate to include:

- a description of the breach

- the type of personal information involved in the breach

- what response the agency or organisation 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).

How to contact the OAIC

Telephone
1300 363 992 (local call cost, but calls from mobile and payphones may incur higher charges)
TTY
1800 620 241 (this number is dedicated for the hearing impaired only, no voice calls)
Post:
GPO Box 5218
Sydney NSW 2001
Facsimile
+61 2 9284 9666
Email
enquiries@oaic.gov.au
Website
www.oaic.gov.au

SHOULD OTHERS BE NOTIFIED?

Great Diagram but cant insert it here?

Appendix B – Contact list: State and Territory privacy contacts

State Records, South Australia
Telephone
(08) 8204 8786
Post
GPO Box 2343 Adelaide SA 5001
Facsimile
(08) 8204 8777
Email
privacy@sa.gov.au
Website
www.archives.sa.gov.au/privacy/index.html