Data Breach Response Plan

Approved 16/09/2019

.au DOMAIN ADMINISTRATION LTD

www.auda.org.au

PO Box 18315
Melbourne VIC 3001

info@auda.org.au

Purpose

The purpose of the auDA Data Breach Response Plan (Plan) is to set out procedures and lines of authority for auDA in the event that auDA experiences a data breach (or suspects that a data breach has occurred). This Plan is intended to enable auDA to contain, assess and respond to data breaches in a timely fashion and to mitigate potential harm to affected individuals.

What is a data breach?

For the purposes of this Plan, a data breach occurs when information held by auDA is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference. In this Plan, the terms 'data' and 'information' are used interchangeably and should be taken to mean both data and information.

A data breach that involves information that is 'personal information' as that term is defined in the Privacy Act 1988 (Privacy Act) (i.e. information or an opinion about an identified individual, or an individual who is reasonably identifiable whether the information or opinion is true or not, or recorded in a material form or not) may also constitute a breach of the Privacy Act, depending on whether the circumstances giving rise to the data breach also constitute a breach of one or more of the Australian Privacy Principles (APPs) or a registered APP code.

Data breaches involving personal information that are likely to cause individuals to be at serious risk of harm must be reported to the affected individual(s) and the Australian Information Commissioner in accordance with the requirements of the Notifiable Data Breaches scheme introduced by the Privacy Amendment (Notifiable Data Breaches) Act 2017.

Data breaches may arise from:

- loss or unauthorised access, modification, use or disclosure or other misuse;
- malicious actions, such as theft or 'hacking';
- internal errors or failure to follow information handling policies that cause accidental loss or disclosure; and
- not adhering to the laws of the states and territories or the Commonwealth of Australia.

Interaction of the Plan with other laws and policies

Assessing and responding to a data breach may involve the consideration of a number of overlapping policies and legal requirements. For example, a data breach may involve:

- criminal activity which may require referral to the Australian Federal Police;
- a security incident which may require consideration of the Australian Government Protective Security Policy Framework and auDA's Security Policy;
- fraud against the Commonwealth; and
- a disclosure of information about auDA by a staff member or contractor that may trigger an investigation under Public Interest Disclosure 2013.

An auDA Executive will determine the appropriate approach to dealing with a data breach, taking into account all of auDA's legal obligations, with advice from the Legal Counsel and/or General Counsel as necessary.

Jurisdictional arrangements

Where jurisdictional stakeholders have been provided with data in accordance with an Information Framework Agreement (IFA), they are required to sign the conditions of data release section of the data request form, and in so doing commit to storing and using the data in accordance with the

obligations outlined. The data breach process set out in this document applies in the case of a data breach, or if the jurisdiction or auDA becomes aware of or suspects that the conditions of the IFA have been breached.

Responding to data breaches

auDA will follow the process set out below and in Attachment A if there is a data breach relating to personal information for registrants, registrars, associate members or employees.

When a data breach has occurred or is suspected to have occurred, auDA will initiate the following process. However, it should be noted that there is no single method of responding to a data breach and in some cases the following steps may need to be modified. Data breaches must be dealt with on a case-by-case basis, by undertaking an assessment of the risks involved, and using that risk assessment to decide the appropriate course of action.

Suspected or known data breach

When an auDA employee or contractor becomes aware or suspects that there has been a data breach, they will comply with the relevant legislation and regulatory requirements as set out in the Act. auDA has an internal operating procedure to address any suspected or knonw data breaches.

Attachment A: Data breach response process

(Reproduced from https://www.oaic.gov.au/privacylaw/privacy-act/notifiable-data-breaches-scheme)

Maintain information governance and security — APP 1 and 11

Entities have an ongoing obligation to take reasonable steps to handle personal information in accordance with the APPs. This includes protecting personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Suspected or known data breach

A data breach is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds.

Contain

An entity's first step should be to **contain** a suspected or known breach where possible. This means taking immediate steps to limit any further access or distribution of the affected personal information, or the possible compromise of other information.

Assess

Entities will need to consider **whether the data breach is likely to result in serious harm** to any of the individuals whose information was involved. If the entity has reasonable grounds to believe this is the case, then it must notify. If it only has grounds to suspect that this is the case, then it must conduct an **assessment** process. As part of the assessment, entities should consider whether **remedial action** is possible.

Organisations can develop their own procedures for conducting an assessment. OAIC suggests a three-stage process:

- **Initiate:** plan the assessment and assign a team or person
- **Investigate:** gather relevant information about the incident to determine what has occurred
- **Evaluate:** make an evidence-based decision about whether serious harm is likely. OAIC recommends that this be documented.

Entities should conduct this assessment expeditiously and, where possible, within 30 days.

If it can't be done within 30 days, document why this is the case.

Take remedial action

Where possible, an entity should take steps to reduce any potential harm to individuals.

This might involve taking action to recover lost information before it is accessed or changing access controls on compromised customer accounts before unauthorised transactions can occur.

If remedial action is successful in making serious harm no longer likely, then notification is not required and entities can progress to the review stage.

NO — **Is serious harm still likely?** — **YES**

Notify

Where **serious harm is likely**, an entity must prepare a statement for the Commissioner (a form is available on the Commissioner's website) that contains:

- the entity's identity and contact details
- a description of the breach
- the kind/s of information concerned
- recommended steps for individuals

Entities must also notify affected individuals, and inform them of the contents of this statement. There are three options for notifying:

- **Option 1:** Notify all individuals
- **Option 2:** Notify only those individuals at risk of serious harm

If neither of these options are practicable:

- **Option 3:** publish the statement on the entity's website and publicise it

Entities can provide further information in their notification, such as an apology and an explanation of what they are doing about the breach.

In some limited circumstances, an exception to the obligation to notify the Commissioner or individuals may apply.

Review

Review the incident and take action to prevent future breaches. This may include:

- Fully investigating the cause of the breach
- Developing a prevention plan
- Conducting audits to ensure the plan is implemented
- Updating security/response plan
- Considering changes to policies and procedures
- Revising staff training practices

Entities should also consider reporting the incident to other relevant bodies, such as:

- police or law enforcement
- ASIC, APRA or the ATO
- The Australian Cyber Security Centre
- professional bodies
- your financial services provider

Entities that operate in multiple jurisdictions may have notification obligations under other breach notification schemes, such as the EU General Data Protection Regulation.

Attachment B

Data Breach Assessment Report

This template is primarily designed to meet the requirements of assessment of data breaches of personal information as defined by the Privacy Act. A data breach involving other kinds of information may require a different approach.

Under the Privacy Act, auDA must notify affected individuals and prepare a statement for the Information Commissioner if the data breach is likely to result in serious harm to any of the individuals whose information was involved. The purpose of this Data Breach Assessment Report is to:

- enable auDA to document its assessment of a data breach;
- to inform the decision of whether to notify affected individuals and/or the Information Commissioner; and
- to inform auDA's review of the data breach and the taking of actions to prevent future breaches.

This assessment must be completed expeditiously and within 30 days if possible.

Description	**Details**
Description of the breach	Provide a short description of the breach, including the date and time the breach was discovered and the duration and location of the breach.
Type of information involved	Insert the type of information involved.
How was the breach discovered?	Insert details about how the breach was discovered, and by whom.
Cause and extent of breach	Insert details about the cause and the extent of the breach.
List of affected individuals	List the affected individuals or describe the class of individuals who are or may be affected by the data breach.
Is the breach likely to result in serious harm to any of the individuals to whom the harm relates?	Evaluate whether the breach is likely to result in serious harm to any of the individuals to whom the information relates, having regard to: • the kind of information involved; • the sensitivity of the information; • whether the information is protected by one or more security measures, and the likelihood of those measures being overcome; • the persons, or the kinds of persons, who have obtained, or who could obtain, the information; and • if a security technology or methodology was used in relation to the information and designed to make the information unintelligible or meaningless to persons who are not authorised to obtain the information, the

	likelihood that persons could circumvent the security technology or methodology. Seek advice from the Privacy Officer if required.
Remedial action	Insert details of the steps auDA has taken to reduce any potential harm to individuals, e.g. by recovering lost information before it is accessed or changing access controls on compromised systems.
Is or will the remedial action result in making serious harm no longer likely?	State whether the remedial action will result in making serious harm no longer likely. If serious harm is no longer likely, auDA is not required to prepare a statement to the Information Commissioner or to notify affected individuals.
Who will be notified of the breach?	[Select from the following options.] [Option 1] auDA has determined that the data breach is likely to result in serious harm to individuals and therefore auDA will: • provide a statement to the Information Commissioner containing a description of the breach, the kind of information concerned and the recommended steps for individuals. • will [select one of the following options] notify all affected individuals / notify affected individuals at risk of serious harm / publish the statement on auDA's website and publicise it [choose this option only if the first two options are impracticable] [Option 2] auDA has determined that notification of the data breach is not required because it is not likely to result in a serious risk of harm to any individuals.
Preliminary recommendations	Include any recommendations on actions that could be undertaken to contain the breach, remediate the breach or prevent future breaches of a similar nature – these recommendations will feed into auDA's comprehensive review of the data breach.
Names of response team members/staff member	Insert the names and roles of response team member/s. The makeup of the response team will be determined by the auDA Management Team, having regard to the skills required to respond to the breach.
Date	Insert date.