DPC G9.1

Personal information data breaches guideline

Purpose

This Guideline has been developed to provide advice to South Australian Government agencies regarding the identification and notification of inappropriate disclosure of personal information held by their agency. Such disclosure will be termed a “Personal Information Data Breach” within this Guideline.

The Guideline

What is Personal Information?

In delivering government services to the community, agencies collect and manage large amounts of information and data, including personal information, on behalf of citizens and other trusted partners.

Personal information is information or an opinion, whether true or not, relating to a natural person, or the affairs of a natural person, whose identify is apparent, or can reasonably be ascertained. A natural person is this context is a living human being[1].

Personal information can include combinations of name, address, date of birth, financial or health details, ethnicity, gender, religion, etc. The personal information held by an agency may be collected in paper form, verbally or through electronic means.

Where it has been identified that there has been a Personal Information Data Breach, agencies must take prompt action to deal with the breach and inform appropriate parties.

How is personal information collected, managed and used by agencies governed?

The collection, management and use of personal information by South Australian Government agencies, is governed by PC012 Information Privacy Principles Instruction. The South Australian *Data Sharing Act 2016* provides boundaries around specific uses of the personal information collected and held by agencies.

The *Commonwealth Privacy Act* (the Privacy Act) does not generally apply to South Australian Government agencies. However, an amendment to the Privacy Act, which comes into effect in February 2018 will see agencies that hold tax file number (TFN) information, being required to

[1] Information Privacy Principles Instruction.

comply with the Commonwealth's Notifiable Data Breaches scheme, but only in respect to TFN information.

Refer to the section titled "Office of the Australian Information Commissioner (OAIC)" in Attachment 3 to this Guideline for further information relating to data breaches involving TFN information.

What is a Personal Information Data Breach and how does it occur?

A Personal Information Data Breach occurs when official information that is not already publicly available, is lost or subjected to unauthorised access, use modification, disclosure or misuse. Personal Information Data Breaches may occur in a number of ways, including accidental loss, internal errors or deliberate actions of trusted employees, theft of physical assets or the theft or misuse of electronic information (e.g. a cyber attack).

How should agencies manage Personal Information Data Breaches?

When a Personal Information Data Breach is evident, the agency should take prompt action to report the breach, identify the risks, notify relevant affected parties and implement remedial action.

Agency Security Plans, developed in accordance with PC030 Protective Security Management Framework (PSMF), should provide guidance and procedures for reporting, recording, and investigating security incidents, which include Personal Information Data Breaches. These procedures should be consistent with the guidance in this document, and more specific policies, guidelines or procedures should be developed if required.

Who do we notify when there has been a Personal Information Data Breach?

When data breaches occur that contain person information, then the Privacy Committee of South Australia should be notified.

The Chief Executive is responsible for the decision on whether to notify parties affected by a data breach. In some circumstances, the Chief Executive may also refer the matter to the relevant Minister.

In general, if a data breach creates a real risk of serious harm to an individual or organisation, the affected parties should be notified.

However, it may not always be appropriate. Providing notification about low risk breaches can cause undue anxiety and de-sensitise individuals to notice. Each incidence needs to be assessed on a case-by-case basis, to determine whether notification is required.

Appended to this Guideline are tools to assist in identification of notification requirements when Personal Information Data Breach has occurred:

Attachment 1 Data Breach Notification Process is an example of a simple data breach notification guide.

Attachment 2 is a Risk Assessment and Notification tool, to assist agencies to determine whether it is necessary to notify individuals or other parties of a Personal Information Data Breach.

Where can I get further advice?

Attachment 3 to this Guideline is a listing of organisations that you may need to notify of a breach or, where you can seek further advice about the management of Personal Information Data Breaches.

Attachments

1 Data Breach Notification Process

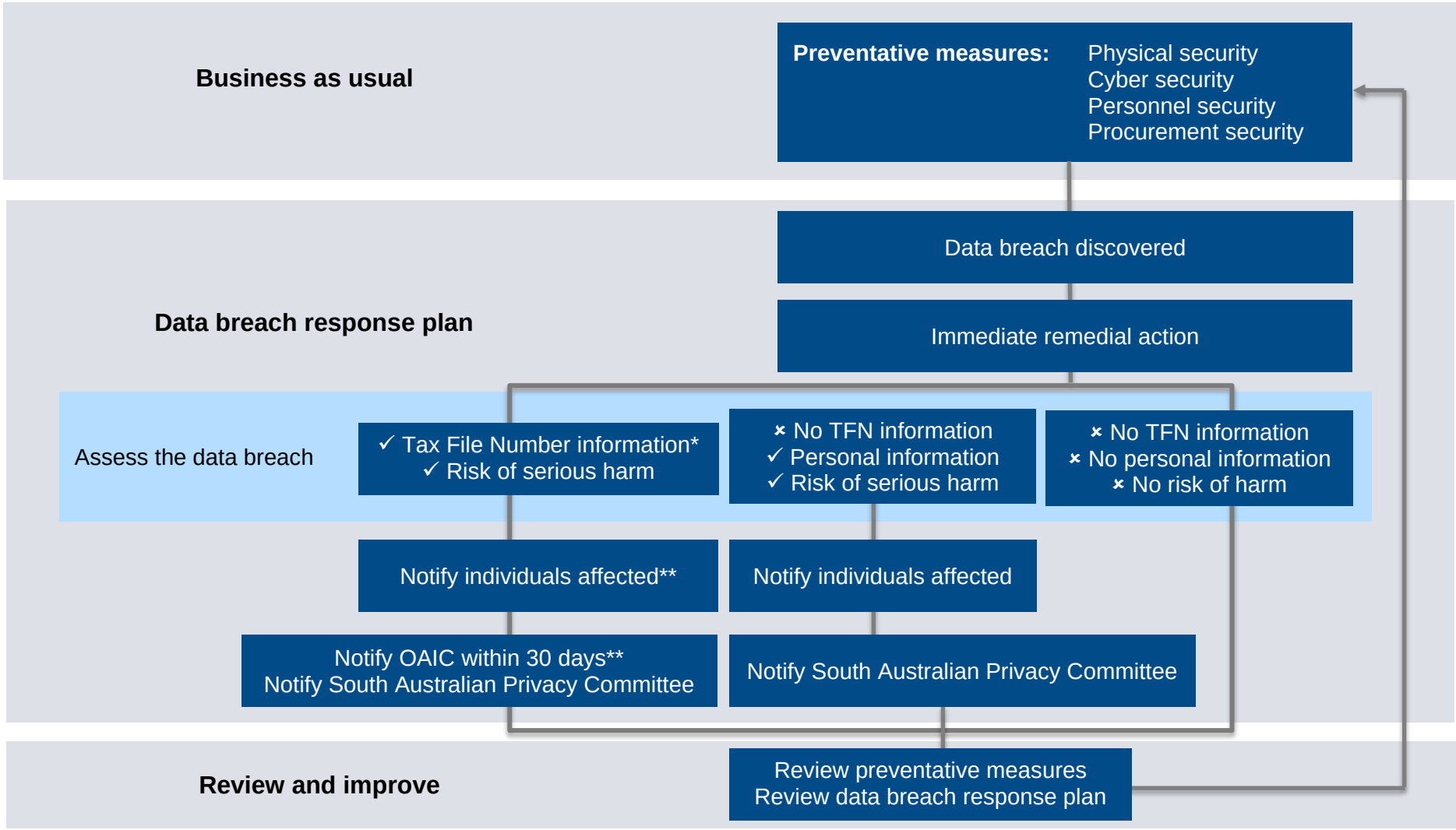
2 Risk Assessment and Notification of Personal Information Data Breaches

3 Contact Organisations for Personal Information Data Breach Advice

References, Links and Additional Information

- PC012 Information Privacy Principles Instruction
- PC030 Protective Security Management Framework
- Protective Security Management Framework
- Office of the Australian Information Commissioner
- Privacy Amendment (Notifiable Data Breaches) Act, 2017

Attachment 1: Data breach notification process



* Tax File Number information is information that connects a Tax File Number with the identity of an individual.

** The *Privacy Amendment (Notifiable Data Breaches) Act, 2017* requires that that notifications to individuals affected and the notification to the Office of the Australian Information Commissioner (OAIC) both contain specific information. See www.oaic.gov.au for more information.

Attachment 2: Risk assessment and notification

Assessing the risk of a Personal Data Breach

Once it is ascertained that a Personal Data Breach is likely to have occurred, agencies should assess the risks associated with the data breach and whether affected parties should be notified.

The following factors should be considered in the risk assessment:

The type of information involved	Does the type of compromised information create a risk of harm? • is it personal, commercial, medical, legal, security classified or other sensitive information? • does the aggregate of information create greater risk of harm? Who is affected by the incident? Are those affected at particular risk? Has tax file number (TFN) information been disclosed?
The context of the information and the incident	What is the context of the information involved? How sensitive is it? What parties have gained unauthorised access to the affected information? Have there been other incidents that could have a cumulative effect? How could the information be used?
The cause and extent of the incident	Is there a risk of ongoing incidents or further exposure of the information? Is there evidence of theft? Was the information targeted? What was the source of the incident? Was it intentional or malicious? Is the information adequately encrypted, anonymised or otherwise not easily accessible? Has the information been recovered? What steps have already been taken to mitigate the harm? Is this a systemic problem or an isolated incident? How many individuals or organisations are affected by the incident?
The risk of harm to those affected	Who is the recipient of the information? What harm to individuals or organisations could result from the breach? Examples of harm include: • identity theft • financial loss • threat to physical safety or emotional wellbeing • loss of business or employment opportunities • damage to reputation or relationships • bullying or marginalisation • insider trading or unfair commercial advantage.
The risk of other harms	Are there any other possible harms that could occur, including to the agency that suffered the incident?

In general, if a data breach creates a real risk of serious harm to an individual or organisation, the affected parties should be notified.

However, it will not always be appropriate. Providing notification about low risk breaches can cause undue anxiety and desensitise individuals to notice. Each incident needs to be assessed on a case-by-case basis to determine whether notification is required.

Prompt notification to those affected in these cases can help them mitigate the damage by taking steps to protect themselves. Agencies should:

- take into account the ability of the individual or organisation to take specific steps to mitigate any such harm
- consider if there any legal, regulatory or contractual obligations to notify
- consider whether it is appropriate to inform third parties such as the police, or other regulators or professional bodies about the data breach incident.

Notifying affected parties

At the point that notification is being considered, the agency should have as complete a set of facts as possible and have completed a risk assessment. Sometimes the urgency or seriousness of the incident dictates that notification should happen immediately, before having all the relevant facts.

When to notify	Those affected should be notified as soon as possible. If it is a criminal matter, check with the law enforcement authorities before notifying so as not to compromise any ongoing investigations.
How to notify	Notify affected parties directly – by phone, letter, email or in person. Indirect notification (e.g. on a website) is only appropriate where direct notification is impossible, unfeasible, or may cause further harm.
Who should notify	Typically, the agency that has a direct relationship with the customer, client or employee should notify those affected. This includes where a breach may have involved handling of information by a third-party service provider or contractor.
Who should be notified	Generally, the individual(s) or organisation affected by the incident should be notified. In some cases, it may be appropriate to notify an individual's guardian or authorised representative on their behalf. The PC012 Information Privacy Principles Instruction should be considered in this process. If the breach contains TFN information then the OAIC may need to be notified under the Notifiable Data Breaches Scheme, and specific requirements apply for notifying individuals affected. See the OAIC website for more information (www.oaic.gov.au).
What should be included in the notification	The information in the notification should help those affected to reduce or prevent the harm that could be caused by the incident. This may include: • a description of the incident

	• the type of information disclosed • what has been done to respond to the incident and reduce harm • assistance available to those affected and steps they can take to reduce harm • sources of information that could assist those affected • contact information for the agency where those affected can get more information or address concerns • whether the incident has been notified to a regulator or other external party • how individuals can lodge a complaint. The wording of the notification may have legal implications, and secrecy obligations could also apply. Agencies should consider seeking legal advice. If the notification is required under the Australian Data Breaches Notification scheme, specific requirements apply (www.oaic.gov.au).
Who else should be notified	Provide details of the data breach and response to the agency Chief Executive and the relevant Minister. Notifying authorities or regulators should not be a substitute for notifying those affected. In some circumstances it is appropriate or necessary to notify the following parties: • State Records • the Privacy Committee of South Australia • South Australian Government Chief Information Security Officer • insurers or others due to contractual obligations • credit card companies or financial institutions • regulatory bodies may have notification requirements • agencies that have a direct relationship with the information exposed (e.g. Medicare in the case of Medicare numbers) • Office of the Australian Information Commissioner

Important considerations

Notifying parties affected by a data breach is considered good practice. It can promote open and transparent government, assist in rebuilding public trust in government institutions and enable individuals and organisations to exercise control over their information, privacy and security.

- The Government of South Australia Information Privacy Principles Instruction regulates the way in which personal information can be collected, used, stored and disclosed by State Government agencies. Personal information is defined as information or an opinion, whether true or not, relating to a natural person or the affairs of a natural person whose identity is apparent, or can reasonably be ascertained, from the information or opinion.
- The decision on how to notify should be made on a case-by-case basis. In some cases, agencies may choose to take additional actions that are specific to the nature of the incident.

- As part of the initial assessment of a security incident, the Agency Security Executive should be immediately informed. Law enforcement, internal investigation units, across government response organisations and other regulatory bodies should also be notified as required by relevant policy or legislation.
- Where law enforcement authorities are investigating the incident, consult the investigating agency before making details of the incident public.

Attachment 3: Contact organisations for advice

In addition to notifying those affected by a data breach, agency data breach response plans should include a list of other parties that may need to be notified. Below is a list of organisations that South Australian Government agencies may be required to notify, or may consider notifying, if a data breach occurs.

Privacy Committee of South Australia

Data breaches involving Personal Information[2] held by South Australian Government agencies should be reported to the Privacy Committee

The Executive Officer of the Committee can also provide general advice on the Information Privacy Principles Instruction and obligations of the reporting organisation

State Records and the Privacy Committee can be contacted on:

- Phone (Business Hours): (08) 8204 8791
- E-mail (Business Hours): staterecords@sa.gov.au
- Website: www.archives.sa.gov.au/

Department of the Premier and Cabinet, Office for Cyber Security

All data breaches that involve information stored or communicated electronically must be reported to the Office for Cyber Security as a cyber security incident. Information on how to lodge a report can be found at https://dpc.sa.gov.au/digital/security

The Office for Cyber Security may also be able to provide advice and assistance on the ICT aspects of managing the data breach and preventative measures.

Report cyber security incidents to the Office for Cyber Security as the Control Agency for Cyber Crisis on:

- Phone (Business Hours): (08) 8226 7513
- E-mail (Business Hours): WatchDesk@sa.gov.au
- Duty Officer (Emergency/Out of Hours number): (08) 8232 3049

South Australia Police

If the data breach may be a result of criminal actions the Police should be notified as soon as practicable.

Delay the notification of those affected by the data breach until advice from the Police is given, as notification may compromise a criminal investigation.

The Police can be contacted on the number below, or visit your local police station:

- Phone (24 hours): 131 444

[2] Personal Information is defined in the Information Privacy Principles Instruction as: information or an opinion, whether true or not, relating to a natural person or the affairs of a natural person whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Office of the Australian Information Commissioner

If the data breach relates to tax file number (information), and it is likely that it will result in serious harm to individuals, the Office of the Australian Information Commissioner (OAIC) must be advised in accordance with the Australian Government's Notifiable Data Breaches scheme (The Scheme).

The Scheme specifies the information that must be included in the notifications for those affected, the timeframe for notification i.e. as soon as practicable within 30 days of the breach being discovered, and the requirement to notify the Australian Information Commissioner of the breach.

Contact details and information on how to report a breach to the OAIC can be found at https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme.

Additional contacts

You may also need to contact:

- **Any other organisation that is the source of the information that was compromised**. For example, if Tax File Numbers or Medicare Numbers were contained the information that was compromised, then the Australian Taxation Office or Medicare respectively should also be notified of the breach.
- **Insurers** such as SAICORP, if required by contractual obligations or to access Cyber Risk Insurance. SAICORP claims and incident reporting contact details:

  Jane Hart – Claims Manager | 8226 3429 | jane.hart@sa.gov.au

  Deborah Machell – Principal Claims Consultant | 8226 2031 | deborah.machell@sa.gov.au
- **Financial institutions** or credit card companies. This may be to assist you in notifying individuals or reducing the impact on those affected.
- **Other internal or external parties**. Consider if any other third parties may have been affected by the breach. For example, if information about a particular government tender process was breached, all organisations that submitted a tender, even if their information wasn't included in the breach, may need to be notified. Some parties to consider include:
  - other internal business units not already notified that may have a need to know (e.g. communications, human resources, senior management group).
  - other government departments that may experience some impact from the breach.
  - unions or other employee representatives, particularly if any employee information was compromised.

Regulatory bodies

Australian Securities and Investment Commission. Companies and registered corporations may have reporting requirements to ASIC.

Australian Competition and Consumer Commission. The ACCC has a role in protecting the interests and safety of consumers and as such they have their own data breach notification requirements. Also consider if individuals affected may contact the ACCC to make a complaint regarding the data breach.

Australian Communications and Media Authority. ACMA have their own data breach reporting requirements if the data compromised includes *Integrated Public Number Database (IPND)* information.

Other regulatory bodies. Your agency may have regulatory bodies specific to your sector that have reporting requirements, or that you should consider notifying. For example, if water licensing information is compromised, the agency may be required to notify water licensing regulatory bodies or boards. The education, infrastructure, health, justice and child protection sectors, in particular, may have specific regulatory bodies that require notification in the case of a data breach.

Document Control

ID	DPC/G9.1
Version	1.0
Classification/DLM	Public-I2-A1
Compliance	Discretionary
Original authorisation date	February 2018
Last approval date	
Next review date	February 2020