STATE SUPER
SAS Trustee Corporation

STC Data Breach Policy

Version 2

4 December 2024

Data Breach Policy

Policy Control Information

Policy Name	STC Data Breach Policy
Policy Owner	General Counsel
Current Version	2
Approval Date	4 December 2024
Next Review Date	4 December 2027 (by Legal team)

Revision History

Version	Prepared By	Reviewed By	Approved By
Version 2	Mark Bendall, Senior Lawyer	Allan Parapuram, General Counsel	CEO/ELC Date:4 December 2024
Version 1	Mark Bendall, Senior Lawyer	Allan Parapuram, General Counsel	CEO Date: 28 November 2023

1. Introduction

This Policy sets out at high-level, how SAS Trustee Corporation (STC) deals with data breaches, including the key controls, systems and processes that it and its contracted service providers have in place, the steps taken to respond to a data breach and to assess whether it is an eligible data breach and its process for reporting an eligible data breach to the NSW Privacy Commissioner.

2. Key definitions

The PPIP Act is the *Privacy and Personal Information Protection Act 1998* (NSW).

The HRIP Act is the *Health Records and Information Privacy Act 2002* (NSW).

An 'eligible data breach' is where:

(a) there is unauthorised access to, or unauthorised disclosure of, personal information held by a public sector agency and a reasonable person would conclude that the access or disclosure of the information would be likely to result in serious harm to an individual to whom the information relates, or

(b) personal information held by a public sector agency is lost in circumstances where:

  (i) unauthorised access to, or unauthorised disclosure of, the information is likely to occur, and

  (ii) if the unauthorised access to, or unauthorised disclosure of, the information were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to an individual to whom the information relates.

An 'affected individual' is an individual specified in subsection (a) or (b)(ii) above. Serious harm is not defined in the PPIP Act. However, the Information and Privacy Commissioner says that it can include physical, financial, or material harm, emotional or psychological harm or reputational harm. The impact of the harm can vary from person to person, but may include:

- financial loss through fraud;
- a likely risk of physical or psychological harm, such as by an abusive ex-partner;
- identity theft, which can affect your finances and/or credit record;
- serious harm to an individual's reputation.

For the purposes of this Policy, personal information is held by a public sector agency if:

(a) the agency is in possession or control of the information, or

(b) the information is contained in a State record in respect of which the agency is responsible under the *State Records Act 1998*.

Personal information is, under the PPIP Act, information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.

Health information, under the HRIP Act, is:

- personal information that is information or an opinion about:
    - the physical or mental health or disability of an individual; or
    - an individual's express wishes about the future provision of health services to him or her; or
    - a health service provided, or to be provided, to an individual, or
- other personal information collected to provide, or in providing, a health service, or
- other personal information about an individual collected in connection with the donation, or intended donation, of an individual's body parts, organs or body substances, or
- other personal information that is genetic information about an individual arising from a health service provided to the individual in a form that is or could be predictive of the health (at any time) of the individual or of a genetic relative of the individual, or
- healthcare identifiers.

For the purposes of this Policy, personal information includes health information. MNDB scheme is the Mandatory Notification of Data Breach scheme pursuant to the PPIP Act.

3. Background

STC is a statutory body created by NSW legislation and continued by the *Superannuation Administration Act 1996* (NSW) (the SA Act). STC is the trustee of various NSW defined benefit public sector super superannuation schemes (the STC schemes), including the:

- State Superannuation Scheme (SSS).
- State Authorities Superannuation Scheme (SASS).
- State Authorities Non-contributory Superannuation Scheme (SANCS).
- Police Superannuation Scheme. (PSS).

STC has various principal functions as set out in the SA Act, including the function of administering the STC schemes. STC has entered into contracts with third parties under which they are each appointed to provide superannuation scheme administration services to an STC scheme or schemes on behalf of STC, which involves the third-party service providers maintaining membership records, including personal information, of STC scheme members (and former members and beneficiaries). It also has contractual relationships with other service providers which involve access to personal information of members of its schemes. STC also holds and manages the personal information of its employees, contract staff and board members.

STC is a public sector agency for the purposes of the PPIP Act and the HRIP Act. It is the PPIP Act that requires STC, as a public agency, to assess any data breach to determine whether it is an eligible data breach and, if it is, to take various other steps such as notifying the Privacy Commissioner of the data breach.

4. What has STC done to mitigate against the risk of a data breach

A data breach involving personal information and/or health information (whether in digital or hard copy) occurs when there is:

- unauthorised access to or unauthorised disclosure personal information or health information held by or for STC; or
- there is a loss of personal information or health information held by or for STC in circumstances that are likely to result in unauthorised access to, or unauthorized disclosure of, the information.

Where the personal information of STC scheme members, former members and beneficiaries, STC employees, contract staff and Board members is held by third parties, those third parties are contractually required to keep that data secure. We also contractually require those third parties to establish and maintain effective data security measures in accordance with industry best practice in order to safeguard the confidential information of STC, which includes the personal information of scheme members, former members and beneficiaries.

STC's third-party service providers have procedures concerning access to, use and disclosure of the personal information of STC scheme members, former members and beneficiaries that enable STC to comply with its obligations and requirements under the PPIP Act and the HRIP Act (and enable those service providers to comply with their obligations under the *Privacy Act 1988* (Cth))

4.1 Cyber-security

The controls and framework that STC has in place in relation to cybersecurity also play a major part in managing the risks to STC's personal information.

STC maintains documented internal policies and procedures that support the organisation's information confidentiality, integrity, availability, and security objectives, and covers management and security of their internal systems as well as operations and systems supporting services provided by relevant third-party providers. These policies and procedures are based on common cyber security frameworks and industry standards.

STC's third-party service providers are contractually required to have rigorous cyber security defences in place, so as to keep the data of STC they hold secure from hackers and other cyber-threats.

4.2 Training and awareness

There are training and awareness-raising requirements for STC staff on induction into the organisation. Attendance is mandatory at annual compliance training sessions which include presentations on information security, records management, codes of conduct and ethics, data risk management and cybersecurity. Each STC staff member also has to confirm annually that they have complied with STC's Code of Conduct and Ethics, which *inter alia* requires them to be aware of and to comply with STC's policies and procedures involving information security, data risk management and cybersecurity.

There are equivalent sessions for Board members.

5. Identification and reporting process for data breaches

Staff members at STC are required, , upon becoming aware of any data breach (whether internal or external) (as defined in this Policy), to immediately notify relevant senior managers within STC.

STC's contracted service providers are contractually required to report data breaches involving STC data, particularly those involving personal information of individuals, to STC within specified timeframes, but in any case as soon as is reasonably practicable.

STC takes steps to, and requires its contracted administration service providers to, immediately make all reasonable efforts to contain any data breach once it or they become aware of the breach.

6. Assessment of data breaches

STC has documented processes to assess whether a data breach is an is an eligible data breach or that there are reasonable grounds to suspect that it is an eligible data breach.

In accordance with s.59H of the PPIP Act, the factors that may be considered to assess if the data breach is an eligible data breach, include:

(a) the types of personal information involved in the breach,

(b) the sensitivity of the personal information involved in the breach,

(c) whether the personal information is or was protected by security measures,

(d) the persons to whom the unauthorised access to, or unauthorised disclosure of, the personal information involved in the breach was, or could be, made or given,

(e) the likelihood the persons specified in paragraph (d):

  (i) have or had the intention of causing harm, or

  (ii) could or did circumvent security measures protecting the information,

(f) the nature of the harm that has occurred or may occur, taking into account the guidance from the Privacy Commissioner about the definition of serious harm (see the Key definitions section of this Policy).

The CEO, or the General Counsel with delegated authority from the CEO, will take reasonable steps to complete this assessment within 30 days. If the CEO or General Counsel forms the view that an assessment cannot reasonably be conducted within 30 days, an extension of time will be approved and STC will notify the Privacy Commissioner.

During the assessment period, STC staff, in conjunction with the service provider involved to the extent necessary, will make all reasonable attempts to mitigate the harm done by the suspected breach.

Under the PPIP Act, the powers to carry out the functions required of STC by the Act are vested in the head of the agency (STC) ie the Chief Executive Officer (CEO). However, the PPIP Act explicitly allows the CEO to delegate the functions provided by the Act to the CEO to a person employed by STC.

STC has a documented Delegations Framework that sets out how various statutory powers provided to STC by the SA Act and the legislation governing the STC schemes are delegated by the STC Board to the CEO or to certain administration service providers and a statutory committee. The STC Board has now included in the Delegations Framework the delegation, with the authority of the CEO provided by the PPIP Act, to the General Counsel of STC of the following functions in the PPIP Act

- Assessment of a data breach as to whether it is an eligible data breach.
- Approval of an extension of the assessment period.
- Decision about whether a data breach is an eligible data breach.
- Notification of an eligible data breach to the Privacy Commissioner and to individuals affected by the breach.
- Maintenance of a data breach incident register.

The General Counsel may use lawyers employed within the STC Legal team to assist in carrying out these delegated functions, but will formally approve or make decisions in exercise of the delegated functions him or herself.

7. Processes in relation to eligible data breaches

7.1 Decision about whether there has been an eligible data breach

Once the assessment has been completed, CEO, or the General Counsel , with delegated authority from the CEO, will decide whether:

- the data breach is an eligible data breach; or
- there are reasonable grounds to suspect that the data breach is an eligible data breach.

If the decision is either that the data breach is an eligible data breach or that there are reasonable grounds to suspect that it is an eligible data breach, then the Privacy Commissioner must be notified of the eligible data breach by the CEO or the General Counsel immediately, using the Data Breach Notification to Privacy Commissioner form https://www.ipc.nsw.gov.au/sites/default/files/2023-10/Form_Data_Breach_Notification_to_the_Privacy_Commissioner_July_2023.pdf

If the data breach is **not** an eligible data breach and there are **not** reasonable grounds to suspect that it is an eligible data breach, then the normal breach remediation process (whether conducted by STC or by the relevant third-party service provider on STC's behalf) should still occur. Any action required to mitigate to the extent possible of any damage or loss suffered by the individual or individuals whose personal information may have been lost or disclosed should be carried out. So should the implementation of any amendments to controls or procedures required to ensure that the breach is remedied and, to the extent possible, will not re-occur.

7.2 Reporting to the Privacy Commissioner

The information that is required to be provided by STC (by the CEO or the General Counsel) to the Privacy Commissioner in relation to an eligible data breach is:

- the name of the public sector agency the subject of the breach (STC);
- if more than 1 public sector agency was the subject of the breach, the name of each other agency and whether STC is reporting about the breach on behalf of the other agencies;
- contact details for a person nominated by STC as the contact person in relation to the breach, or
- a person nominated by the agency for the individual to contact about the breach;
- the date the breach occurred;
- a description of the breach;
- a description of the personal information that was the subject of the breach;
- how the breach occurred;
- the type of breach that occurred (unauthorised disclosure or unauthorised access or loss of information or other);
- the amount of time the personal information was disclosed for;
- whether the breach is a cyber incident and if so, details of the cyber incident;
- the estimated cost of the breach to STC;
- the total number, or estimated total number, of individuals:
    - affected or likely to be affected by the breach;
    - notified of the breach;
- how and when the individuals who have been notified of the breach were notified and whether they were advised of the complaints and internal review procedures under the PPIP Act;
- remedial actions that have been taken or are planned to ensure the personal information is secure, or to control or mitigate the harm done to the affected individuals;
- recommendations made to affected individuals about the steps an individual should take in response to the eligible data breach;
- any other bodies (ie the Police) that STC has notified about the breach.

7.3 Reporting to affected individuals

STC is required by the PPIP Act to notify the individuals affected by an eligible data breach about the data breach as soon as is practicable after the decision is made that an eligible data breach has occurred. The information that is required to be provided by STC (CEO or the General Counsel) to each affected individual is as follows:

- the name of the public sector agency the subject of the breach (STC);
- the date the breach occurred;
- a description of the breach;

- the personal information of the affected individual that was the subject of the breach;
- how the breach occurred;
- the type of breach that occurred (unauthorised disclosure, unauthorised access or loss of information or other);
- the amount of time the personal information was disclosed for;
- remedial actions that have been taken or are planned to ensure the personal information is secure, or to control or mitigate the harm done to the affected individual;
- recommendations about the steps the affected individual should take in response to the eligible data breach;
- information about procedures under the PPIP Act for making a privacy-related complaint to the Privacy Commissioner and how to seek an internal review of STC's conduct in relation to the breach;
- if more than 1 public sector agency was the subject of the breach, the name of each other agency;
- contact details for a person nominated by STC as the contact person for the individual to contact in relation to the breach.

7.4 Public Notification Register

STC will always take all reasonable steps to directly notify any or all the individuals affected by an eligible data breach but if it is not reasonably practicable to do so, STC staff will prepare and maintain on the State Super website for at least 12 months, in what will be known as the STC Public Notification Register, the following information about the breach:

- the date the breach occurred;
- a description of the breach;
- a description of the personal information that was the subject of the breach (but without disclosing any personal information of any affected individual);
- how the breach occurred;
- the type of breach that occurred (unauthorised disclosure, unauthorised access or loss of information or other);
- the amount of time the personal information was disclosed for;
- remedial actions that have been taken or are planned to ensure the personal information is secure, or to control or mitigate the harm done to any affected individual;
- recommendations about the steps any affected individual should take in response to the eligible data breach;
- information about procedures under the PPIP Act for making a privacy-related complaint to the Privacy Commissioner and how to seek an internal review of STC's conduct in relation to the breach;
- if more than 1 public sector agency was the subject of the breach, the name of each other agency;
- contact details for a person nominated by STC as the contact person for the individual to contact in relation to the breach.

No information should be published in the Public Notification Register that contains personal information of any individual or that may prejudice STC's functions.

7.5 Notification to third parties

STC will also make sure to provide the information about the breach where it is necessary to be notified to any third parties in accordance with any applicable law, such as:

- the Police;
- STC's insurer (Treasury Managed Fund);
- NSW Treasury;
- other NSW agencies that may have a direct relationship with the information that is lost/stolen, such as State Records NSW or Museums of History NSW.

7.6 Post-breach review and evaluation

STC considers that the post-breach review and evaluation is important so that the root causes of the breach are identified and to remediate and rectify the breach and any adversely impacted members involved. This will also include consideration and establishment of preventative measures to reduce the chances of future reoccurrence.

7.7 Eligible data breach incident register

STC (the CEO or the General Counsel) will maintain an internal register for eligible data breaches. The register must include details of the following, where practicable, for all eligible data breaches:

- who was notified of the breach;
- when the breach was notified;
- the type of breach;
- details of steps taken by STC to mitigate harm done by the breach;
- details of the actions taken to prevent future breaches;
- the estimated cost of the breach.

8. Review of Policy

The STC Legal team will review this Policy triennially (or more frequently as required) and will submit the reviewed, and if necessary updated version to the Executive Leadership Committee (ELC) for approval.