NSW Treasury

NSW Treasury Data Breach (Privacy) Policy

TIPP 5.20

14 April 2024

NSW GOVERNMENT

Acknowledgement of Country

We acknowledge that Aboriginal and Torres Strait Islander peoples are the First Peoples and Traditional Custodians of Australia, and the oldest continuing culture in human history.

We pay respect to Elders past and present and commit to respecting the lands we walk on, and the communities we walk with.

We celebrate the deep and enduring connection of Aboriginal and Torres Strait Islander peoples to Country and acknowledge their continuing custodianship of the land, seas and sky.

We acknowledge the ongoing stewardship of Aboriginal and Torres Strait Islander peoples, and the important contribution they make to our communities and economies.

We reflect on the continuing impact of government policies and practices and recognise our responsibility to work together with and for Aboriginal and Torres Strait Islander peoples, families and communities, towards improved economic, social and cultural outcomes.

Artwork:
Regeneration by Josie Rose

Version	
Document number TIPP 5.20	Version number: 1
Original issue date	14 April 2024
To be reviewed	April 2026

Contact Information
Department: NSW Treasury
Branch: Governance, Ethics, & Integrity
Division: Office of General Counsel
Email: governance@treasury.nsw.gov.au

General inquiries concerning this document should be initially directed to:
Governance, Ethics, and Integrity Branch, NSW Treasury; governance@treasury.nsw.gov.au.

Purpose

This policy provides an overview of the mechanism for NSW Treasury to respond to and manage privacy data breaches. Privacy data breaches might be non-technical in nature (i.e. human error) or have a cyber security component (i.e. a cyber incident resulting in a privacy data breach). It is important to note that the foundations of this policy apply to privacy rather than cybersecurity. Matters relating to the technical aspects of cybersecurity and the policies surrounding the governance of Information Technology (IT) systems should be dealt with under NSW Treasury's IT, Risk and Information policies and procedures.

When an incident involves the potential exposure of 'personal information', it becomes a privacy incident and possibly a notifiable 'data breach' under the Privacy and Personal Information Protection Act 1998 (NSW) (PPIP Act).

NSW Treasury will follow a risk management approach to dealing with security and privacy threats. Privacy data breaches are to be evaluated on a case-by-case basis and actions taken according to an assessment of risks and responsibilities in the particular circumstances. This document forms part of NSW Treasury's adherence to its responsibilities under privacy and other laws.

Scope

This policy applies to all NSW Treasury employees, contractors, consultants, and others who collect personal information on behalf of NSW Treasury.

This policy applies to personal information that is 'held' by NSW Treasury (whether in digital or hard copy).[1] NSW Treasury's legal obligations extend to personal information that is either —

(a) in the possession and control of NSW Treasury[2]

(b) contained in a state record in respect of which NSW Treasury has responsibility under the *State Records Act 1988*,[3] in the sense that it is entitled to control (including by placing it in the possession or custody of another person or entity or having the legal or practical power to deal with the personal information).[4]

For example, while a record containing personal information may be physically in the possession of another entity or agency, NSW Treasury may retain authority to determine what is done with the records.[5] In this case, NSW Treasury would jointly 'hold' that information with the other entity or agency.

Systems, Processes, Reporting and responding to Data Breaches (Privacy)

For a guide of the systems used in NSW Treasury and a step-by-step guide as to how NSW Treasury will report on and respond to a Data Breach, refer to the **Data Breach (Privacy) Response Plan and Procedure TIPP 5.20a** (available internally only).

[1] See IPC guidance at https://www.ipc.nsw.gov.au/guide-mandatory-notification-data-breach-scheme-guide-managing-data-breaches-accordance-ppip-act.

[2] PPIP Act section 59C(a).

[3] PPIP Act section 59C(b).

[4] Sections 5 and 6 of the *State Records Act 1988* (NSW); see also IPC guidance at https://www.ipc.nsw.gov.au/guide-mandatory-notification-data-breach-scheme-guide-managing-data-breaches-accordance-ppip-act.

[5] See IPC guidance at https://www.ipc.nsw.gov.au/guide-mandatory-notification-data-breach-scheme-guide-managing-data-breaches-accordance-ppip-act.

Related Documents and applicable policies

This Data Breach (Privacy) Policy should be read in conjunction with the PPIP Act, the Privacy Management Plan TIPP 5.19 and the following policies:

- NSW Treasury's online Privacy Statement
- Code of Ethics and Conduct TIPP 2.05
- Records Management Framework TIPP 4.01
- Information Security Policy TIPP 4.08
- Incident Response Procedures TIPP 4.22
- Risk Management Framework TIPP 5.01
- Compliance Incident Framework TIPP 5.14
- Data Breach (Privacy) Response Plan and Procedure TIPP 5.20a (available internally only)

Personal information held by third parties

NSW Treasury's obligations under the PPIP Act's Mandatory Notification Data Breach scheme extend to all information over which it has a right or entitlement to deal with. This includes all personal and health information that is placed in the possession or control of a third party such as an external service provider (for example, IT solutions).

Contractual arrangements should include third-party assurances to assist NSW Treasury manage third-party data breaches (including in relation to notification and remediation).

Key Definitions

Data breach means:

An incident in which there has been **unauthorised access to, unauthorised disclosure of, or loss of, personal information** held by (or on behalf of) NSW Treasury.

A data breach may occur as a result of malicious action, systems failure or human error. It may also be caused by a misconception about whether a particular act or practice is permitted.

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, businesses and agencies. Although there is a lot of overlap between information security incidents and data breaches, they are not exactly the same. Some cybersecurity incidents will not involve or impact anyone's personal information. Some data breaches will involve only hard copy information such as paper files.

Personal information means:

Information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.

This will include information about our staff (including contractors and secondees), customers, clients, stakeholders, residents, suppliers, and other contacts. The information could come from businesses and individuals involved in NSW Treasury's programs, schemes, forums, events, and grants as well as those making a complaint, enquiry, comment, or suggestion, making a formal access application under the *Government Information (Public Access) Act 2009* (NSW), registering for NSW Treasury communications, or making a public submission.

It can include details such as name, address, phone number, email address, date of birth, tax file number, health and medical records, employee records, identification documents, digital images, correspondence records, licence details, or criminal records.

Individuals may still be identifiable even if steps have been taken to de-identify information (for example, removing direct identifiers or aggregating data). As such, it is prudent to treat de-identified information as personal information in the event of a data breach.

However, personal information does not include any of the following:

- information relating to a person who has been dead for more than 30 years
- information contained in a publicly available publication
- information or an opinion referring to a person's suitability for employment as a public sector official.

For more information on the types of personal information held by NSW Treasury, please see the **Privacy Management Plan and Guidelines (TIPP 5.19).**

Health information means:

Any personal information which may include information or opinions about the physical or mental health or disability of any individual, or provision of health services to them.

It also includes genetic information that is or could be predictive of the health of a person and any personal information that was collected to provide, or in providing, a health service or in connection with donation of body parts, organs or body substances.

Notifiable data breach means:

A data breach which meets certain criteria, such as to trigger a legal requirement to notify the affected individuals, and/or appropriate regulator.

Low risk data breach means:

A loss or exposure of aggregated data only, or of individual level data in circumstances where it is reasonably believed that no real harm could occur.

Medium risk data breach means:

A loss or exposure of personal information where it is reasonably believed that the third-party recipient does not have malicious intent, and that the data is somewhat protected.

High risk data breach means:

It is reasonably believed that the data breach is **likely to result in serious harm** to one or more of the individuals to whom the information relates.

A 'high risk' data breach will be a 'notifiable' data breach unless it falls under one of the exceptions to the notification rules.

Serious harm means:

'Serious harm' occurs where there is a real and substantial detrimental effect to the individual.[6] It includes such things as serious physical, psychological, emotional, economic, financial, or reputational harm.

Likely to result in serious harm means:

'Likely' means a real and not remote chance of the risk of serious harm to an individual.

This is an objective assessment, determined from the viewpoint of a reasonable person in NSW Treasury's position who is properly informed by information either immediately available to them or obtained following reasonable inquiries or assessments of the data breach.

To help assess the likelihood that an individual might suffer serious harm if their personal information was lost, or subject to unauthorised access or unauthorised disclosure, there are a number of factors to consider.

[6] See IPC guidance at https://www.ipc.nsw.gov.au/guide-mandatory-notification-data-breach-scheme-guide-managing-data-breaches-accordance-ppip-act.

Summary of Key Responsibilities

Division	Key Responsibilities for Privacy Data Breaches
OGC (GE&I)	• The administration of this plan in accordance with the PPIP Act and associated regulations and policies. • Management and review of the actions required by NSW Treasury in response to a privacy data breach. • Reporting and liaising with regulatory and other stakeholders including working with the communications teams within NSW Treasury. • Assessment of risk and ensuring compliance through assurance testing, audits, and other means of ensuring the controls are robust and obligations adhered to by NSW Treasury staff.
Information Technology Division (IT)	• Provide assistance, expert advice, and access to systems in the event of a privacy data breach involving cybersecurity. • Provide expert advice and concurrence in the event that NSW Treasury needs to exempt itself from certain reporting obligations.
OGC (Risk, Compliance & Audit)	• Ensure that all identified incidents are recorded accurately and completely. • Provide advice on impact and associated risk and control failures in partnership with GE&I. • Review and approve incidents when signed off by incident owner.
All staff, volunteers, contractors and contingent labour	• Handle personal information in accordance with the PPIP Act • Take steps to ensure external stakeholders comply with our privacy requirements • Report all breaches and suspected breaches • Assist OGC teams in investigating and assessing breaches, and with any internal reviews that result.

How do I report?

You must report the suspected privacy data breach immediately, either in person or by phone call, to the Privacy Coordinator:

Lead Associate Director, Governance, Ethics & Integrity.

Telephone: 02 9273 3915

You must then confirm your report in writing, by email to:

governance@treasury.nsw.gov.au

and complete and submit the Privacy Data Breach Assessment (PDBA) form.

You must log the suspected data breach immediately, in line with the NSW Treasury Incident Management Policy and Risk Management Frameworks.

What happens after reporting?

Depending on the nature of the breach, privacy legislation might consider it a 'notifiable data breach', meaning that the appropriate regulator and affected individuals (with very few exceptions)[7] must be notified. The Privacy Coordinator will make an assessment about this, in accordance with the Data Breach Response Process outlined below.

Even if you have contained the breach (for example, retrieved a stolen laptop or lost hard-copy files), you must still notify the Privacy Coordinator and submit a report (PDBA form). The Privacy Coordinator will assess any residual risk, and they can also consider whether further action is needed to avoid a similar occurrence.

If the Privacy Coordinator thinks the suspected data breach is likely to result in serious harm to any individual, they must report it immediately to the Leadership Team.

[7] See sections 59S through 59X of the PPIP Act, and the IPC guidance at https://www.ipc.nsw.gov.au/fact-sheet-mandatory-notification-data-breach-scheme-exemptions-notification-requirements.

Staff training and awareness

To ensure that NSW Treasury staff are aware of their responsibilities under this policy and in relation to data breaches, NSW Treasury will:

- publish this policy and additional material in a prominent place on the NSW Treasury intranet and website
- introduce the policy during staff induction with training provided as required, including through e-learning modules
- provide refresher, specialised and on-the-job training for data breaches, including on privacy and cyber principles, the identification and management of data breaches, and current threat trends
- prepare and provide targeted training to those in high-risk roles
- highlight this policy annually during Privacy Awareness Week
- provide briefing sessions on data breaches at appropriate management forums.

52 Martin Place
Sydney NSW 2000

GPO Box 5469
Sydney NSW 2001

W: treasury.nsw.gov.au

NSW GOVERNMENT