Tackling data privacy and security – current landscape, risks, and future initiatives

Presentation to the 9th Annual Australian Data Summit
30 March 2023

Samantha Gavel
Privacy Commissioner

information and privacy commission
new south wales

About the Privacy Commissioner

The NSW Privacy Commissioner:

- is an independent voice on privacy in NSW
- provides advice to the NSW Parliament, the NSW Attorney General, and the Minister for Customer Service and Digital Government, Minister for Small Business, and Minister for Fair Trading
- oversees NSW laws that protect personal and health information under PPIP & HRIP Acts

NSW GOVERNMENT

New technologies mean:

- Easier & faster collection of data
- Large scale collection
- Digital innovation
- **New privacy and cyber security challenges**

Development of a digital government:

- New digital services
- Increased data sharing
- Data analytics and data matching
- Machine learning
- AI and Internet of Things technology

NSW examples:

- Digital Drivers Licence
- Mobile Phone Detection Cameras

COVID-19 and Privacy

Consideration of privacy issues in NSW:

- Sharing and use of data to inform the State Government's pandemic response and provide information to the public
- Development of COVID check-in tool by the NSW Department of Customer Service
- Data breaches resulting from increased malicious cyber security activity during the pandemic
- Collection of Vaccination Information

- The Optus and Medibank cyber breaches have potentially exposed the personal information of millions of Australians
- Lessons from these breaches include the need to:
  - Minimise the collection of personal information
  - Retain personal information only as long as it is needed
  - Dispose of personal information securely when no longer needed
- Importance of robust data breach response plan and stakeholder communication plan
- Challenges and risks in obtaining proof of identity and holding identity documents
- The significant cost of data breaches

Retention and Security of Personal Information

Privacy and Personal Information Protection Act 1998 (NSW)

S 12: A public sector agency that holds personal information must ensure -

(a) that the **information is kept for no longer than is necessary** for the purposes for which the information may lawfully be used, and

(b) that the **information is disposed of securely** and in accordance with any requirements for the retention and disposal of personal information, and

(c) that the information is protected, by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised access, use, modification or disclosure, and against all other misuse.

ACSC Annual Cyber Threat Report 2022

- An increase in financial losses due to Business Email Compromise to over **$98 million**; an **average loss of $64,000** per report.
- A rise in the average cost per cybercrime report to over **$39,000** for small business, **$88,000** for medium business, and over **$62,000** for large business; an average increase of 14 per cent.
- A **25 per cent increase** in the number of publicly reported software vulnerabilities (Common Vulnerabilities and Exposures – CVEs) worldwide.
- Over **76,000 cybercrime reports**; an increase of 13 per cent from the previous financial year.

IBM-Ponemon Institute Cost of a Data Breach Report 2021

- The average Australian data breach **cost $3.7m** (US$2.82m) – up 31 per cent from $2.8m (US$2.15m) the previous year.
- Australian companies took **311 days on average** to detect and contain data breaches.
- An average of **23,800 records** stolen per Australian breach – costing $169 per record on average.
- The report found that a combination of actions and activities by organisations was the most effective way for an organisation to reduce the cost of a breach.
- Activities that proved effective in reducing the cost of a breach included creating an **incident response team** and **testing cyber response plans**.

Service NSW cyber incident

- In May 2020, Service NSW experienced a significant cyber incident which had compromised the email inboxes of **47 staff members**.
- Service NSW organised for a forensic analysis of the **3.8 million documents exposed** in the breach.
- Personal information of **104,000 customers and staff** was exposed in the incident.
- The Privacy Commissioner was updated by the Department of Customer Service regarding the extent of the breach and the actions being taken to notify and support customers affected.
- The Minister for Customer Service requested the NSW Auditor General to conduct a performance audit to assess how effectively the agency was handling personal information to ensure its privacy. The report provides several lessons and learnings for agencies and organisations.

Service NSW Cyber Incident

Lessons from breach

- Implement Multi-Factor Authentication
- Don’t use email for transferring information or for document storage
- Secure storage and regular deletion of personal information
- Purge email deleted items folders on a regular basis
- Risks of legacy systems and processes
- The estimated cost of the breach was $25 to $35 million

Keeping data secure

- A whole of organisation data governance framework is required.
- Privacy protective organisational culture, led from the top down.
- Understand what information you hold, how long you need to retain it, where is it held, who has access to it and how it will be securely disposed of.
- Tools include Privacy-by-Design, Privacy Impact Assessments and Privacy Enhancing Technology.
- A data breach response plan which includes processes and procedures to manage and mitigate a data breach.
- Regular privacy and cyber security training for staff and contractors.

Privacy by design

Privacy should be considered at all stages of the project, from conception through to the development and implementation phases.

By developing an organisation-wide awareness of privacy, a privacy by design approach shifts the focus to preventing privacy-related issues, rather than simply complying with privacy laws.

Privacy and Personal Information Protection Amendment Bill 2022

- The PPIP Amendment Bill passed both houses of NSW Parliament on 16 November and was assented to on 28 November 2022.
- Amendments to come into effect 12 months after assent on **28 November 2023**.
- Key changes include:
  - **Creation of a Mandatory Notification of Data Breach (MNDB) Scheme** in which NSW public sector agencies bound by the PPIP Act will need to notify the Privacy Commissioner and affected individuals of data breaches involving personal or health information likely to result in serious harm
  - applying the PPIP Act to all **NSW state-owned corporations** that are not regulated by the Commonwealth *Privacy Act 1988*
  - repealing s117C of the *Fines Act 1996* to ensure that all NSW public sector agencies are regulated by the same mandatory notification scheme.

Privacy and Personal Information Protection Amendment Bill 2022

Preparing your agency for the scheme:

- Establish and clarify roles & responsibilities
- Review and update your Privacy Management Plan
- Prepare and publish a Data Breach Policy
- Review and update relevant policies and procedures
- Establish an incident register
- Establish a public notification register

E-Newsletter

The IPC is releasing a new bi-monthly e-newsletter from April 2023 to update practitioners about new resources and information relating to the MNDB Scheme.

Subscribe for updates via the IPC website.

Privacy and Personal Information Protection Amendment Bill 2022

The IPC website has a dedicated MNDB page which will be regularly updated in the lead up to the scheme: www.ipc.nsw.gov.au/privacy/MNDB-scheme

Upcoming guidance:

- **NEW** Fact Sheet for agencies: Exemptions from notification to affected individuals
- Guide to preparing a data breach policy (May 23)
- Fact Sheet for citizens: What is the MNDB Scheme (May 23)
- Fact Sheet for citizens: Your rights under the MNDB Scheme (May 23)
- Guide for agencies: MNDB Scheme (Jun 23)
- Guideline: Assessing an eligible data breach (Aug 23, Minister approval)
- Guideline: Exemption under s 59W (health and safety) (Aug 23, Minister approval)
- Guideline: Exemption under s 59X (cybersecurity) (Aug 23, Minister approval)

Connect with us

www.ipc.nsw.gov.au

ipcinfo@ipc.nsw.gov.au

1800 472 679

/company/information-and-privacy-commission-nsw

@IPCNSW

/InformationandPrivacyCommissionNSW

www.youtube.com/user/IPCNSW

information and
privacy commission

new south wales