Mandatory Data Breach Disclosure
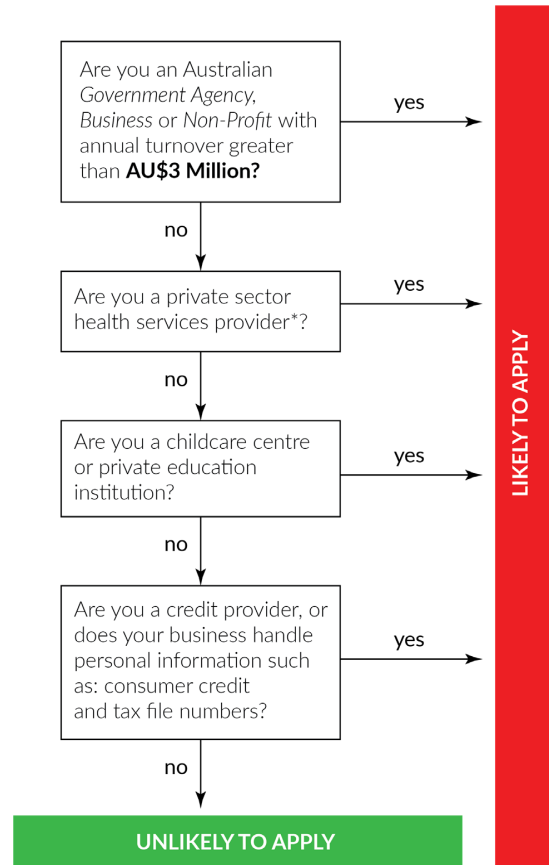
Whitepaper

Equipping your business for privacy act compliance with snare

The Australian Privacy Act, introduced in the late 20th century, endeavors to protect the privacy of Australians. As technology has evolved so too has the meaning of what it is to keep information private – necessitating changes to the Act. The latest amendment to the Act introduces new regulations in Australia around how businesses handle personal information – the Privacy Amendment (Notifiable Data Breaches) Act 2017. This new law introduces a Notifiable Data Breaches (NDB) Scheme which requires all businesses that fall under the jurisdiction of the Office of the Australian Information Commissioner (OAIC) to take reasonable steps to: (i) notify the OAIC and affected individuals if they become aware of a breach that is likely to result in serious harm to the individuals affected; and (ii) to conduct a complete assessment of the breach within 30-calendar-days from the day the breach is suspected.

According to the Ponemon Institute it takes an average of 66-days to contain a data breach[1]. It is necessary, therefore, for businesses to invest heavily in software that can automate the detection and investigation of breaches to ensure their Privacy Act Compliance.

```
┌─────────────────────────┐
│ Are you an Australian   │────── yes ──────►  ┐
│ Government Agency,      │                     │
│ Business or Non-Profit  │                     │
│ with annual turnover    │                     │
│ greater than AU$3       │                     │
│ Million?                │                     │
└───────────┬─────────────┘                     │
          no                                    │
┌───────────▼─────────────┐                     │
│ Are you a private sector│────── yes ──────►   │  LIKELY TO APPLY
│ health services         │                     │
│ provider*?              │                     │
└───────────┬─────────────┘                     │
          no                                    │
┌───────────▼─────────────┐                     │
│ Are you a childcare     │────── yes ──────►   │
│ centre or private       │                     │
│ education institution?  │                     │
└───────────┬─────────────┘                     │
          no                                    │
┌───────────▼─────────────┐                     │
│ Are you a credit        │────── yes ──────►   ┘
│ provider, or does your  │
│ business handle         │
│ personal information    │
│ such as: consumer credit│
│ and tax file numbers?   │
└───────────┬─────────────┘
          no
┌───────────▼─────────────┐
│   UNLIKELY TO APPLY     │
└─────────────────────────┘
```

*a traditional healthcare provider (hospital, medical practitioner, pharmacy), complimentary therapists (e.g. naturopaths), a gym or weightloss clinic.

WHAT'S HAPPENING?	WHY IT MATTERS?	HOW CAN SNARE HELP?
On February 22, 2018 the amendments to the Australian Privacy Act came into effect. Changing what is required of businesses who handle sensitive personal information. The updated regulation calls for mandatory reporting of breaches and enforces a 30-calendar-day investigation period.	A failure to abide by the Privacy Amendment (Notifiable Data Breaches) Act of 2017 can result in hefty financial penalties of up to AU$360,000 for individuals, and up to AU$1.8 million for organizations.	Snare is a log management platform that can greatly aid in the detection of security breaches by centrally collecting, monitoring and managing log data and user activity. Allowing breach investigations to occur more efficiently, and greatly supporting your Privacy Act compliance.

WHAT ARE REASONABLE STEPS?

The OAIC identifies a mixture of administrative (policies, procedures) and technical controls that businesses should deploy in order to remain compliant, within the following nine categories[2]:

1. Governance, culture and training

2. Internal practices, procedures and systems

3. ICT security

4. Access security

5. Third-party provider access controls

6. Data breaches

7. Physical security

8.   Destruction and de-identification

9.   Standards

RECOMMENDED BREACH INVESTIGATION PROCESS

The OAIC recommends that businesses undertake a three-stage process to investigate a breach:

**Initiate** to determine if an assessment is needed.

Investigate the breach (what information is

affected, who had access, what is the impact).

Evaluate whether the breach is an 'eligible' breach

A COMPREHENSIVE SECURITY ECOSYSTEM TO SUPPORT PRIVACY ACT COMPLIANCE

Snare provides a unified management platform in the Snare Agents and Snare Central, which help to ensure your compliance with the Privacy Act - offering multiple security management capabilities with pre-built, comprehensive reporting, dashboards and threat identification.

Snare Agents gather disparate events and logs, parses the information and correlates the data in a central platform. This provides an efficient record of your logs, that can be forwarded to Snare Central or another third-party SIEM for detailed forensic analysis. With Snare Agents historical data can be stored and easily accessible in the event that a breach is suspected and investigations must be undertaken. Ultimately the Snare platform can mitigate the risk exposure in you ICT infrastructure.
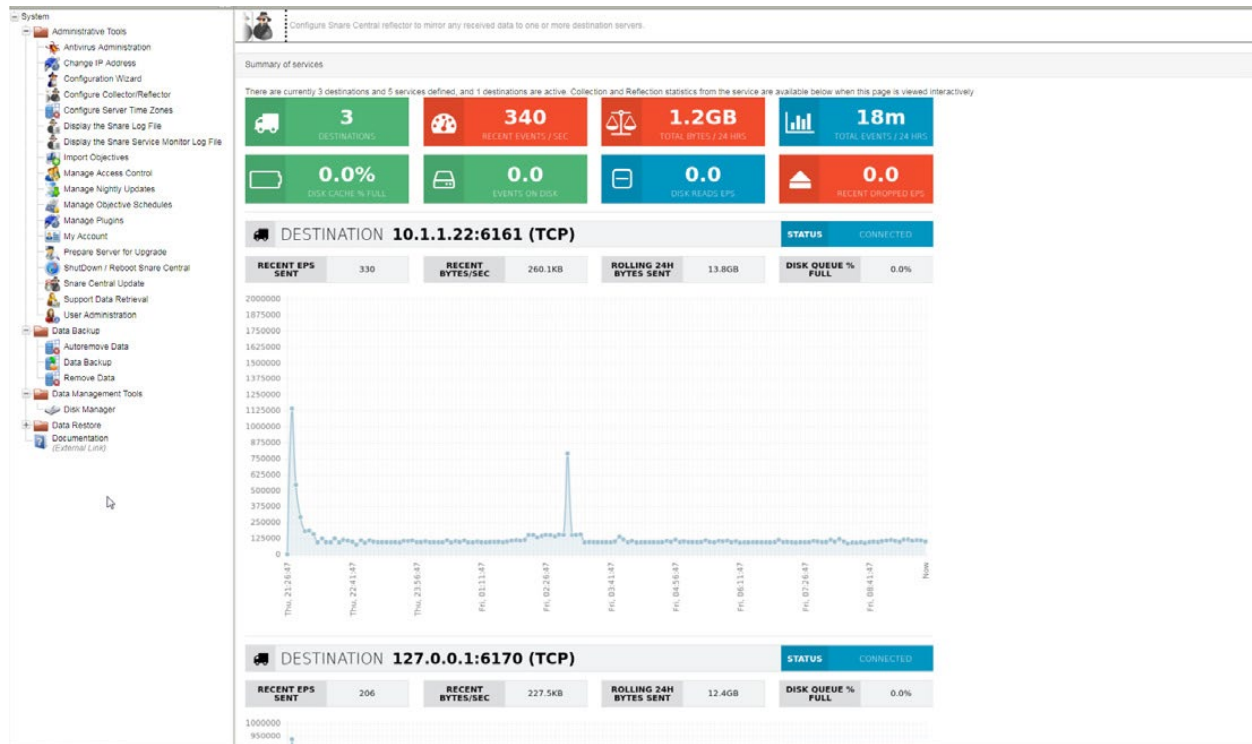
THE SOLUTION

The Snare Agents, Snare Central and the Snare Reflector can be combined to collect and monitor activity across distinct areas, including:

- User movements through the IT environment - access to systems, applications, services and file access; and

- Data integrity monitoring Identification of system changes; including configuration or system policy changes
- Extractions of data from the system; monitoring removable media usage, and file transfers to third-party applications and system logs

With the Snare reflector, you can reflect your logs to third-party SIEMs, or other analytical platforms for processing. However, the powerful reporting and alerting facilities of Snare Central, combined with the flexible collection

and filtering abilities of the Snare Agents, can provide you with the capacity to meet the Privacy Act requirements. The platform detects critical issues, provides timely notifications, and empowers the security team to conduct comprehensive forensic investigations.

Snare can provide real-time triggers from threshold and alerts on a pattern of activity, or match on a number of specific events. Whilst, also facilitating data access reviews for PII via file activity monitoring and database query tracking. Data is your business's most valuable asset, and the central focus of the Privacy Act. Thus, it is crucial that you understand it, manage it and protect it. The integration of an effective collection, analysis and reporting platform in Snare, can support you in meeting the Privacy Act requirements.

ADDITIONAL RESOURCES:

To find out more about how Snare can help you, visit:

http://www.snaresolutions.com/

For more information about the Privacy Act, visit:

https://www.legislation.gov.au/Details/C2017A00012

https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme

https://www.oaic.gov.au/resources/agencies-and-organisations/guides/data-breach-preparation-and-response.pdf