A BRIEF GUIDE

to the ICT Security Controls Required by the Australian Privacy Principles and Mandatory Data Breach Notification Scheme

On 13 February 2017 the Senate passed the Privacy Amendment (Notifiable Data Breaches) Bill establishing a Mandatory Data Breach Notification Scheme in Australia. The purpose of which is to protect the rights of individuals and strengthen community trust in businesses and agencies.

This amendment to the Australian Privacy Act 1988 (Privacy Act) gives life to the Mandatory Data Breach Notification Scheme (the Scheme) which came into effect on 22 February 2018. The scheme has been in place for three years now and we have seen multiple breach notifications been made to the Office of the Australian Information Commissioner (OAIC) each quarter.

Many organisations do not either understand their obligations under this scheme or simply do not know how to comply. The rest of this paper tries to raise awareness towards this.

The Privacy Act provides significant obligations for the protection of Personal Information held by Australian organisations (APP entities) and material financial penalties of up to $500,000 for a person other than a body corporate. Fines for a body corporate – the greater of either: $10,000,000; the value of any benefit the relevant court has determined of the body corporate, or any body corporate related to it, obtained directly or indirectly that is reasonably attributable to the contravention, multiplied by three; or if the court cannot determine the value of that benefit, 10% of the annual turnover of the body corporate during the 12-month period ending at the end of the month in which the contravention happened or began. 'APP Entities' are defined Australian Government agencies (and the Norfolk Island administration) and organisations with an annual turnover more than $3 million, subject to some exceptions and a range of small businesses (see ss 6D and 6E of the Privacy Act). State Government agencies are not generally governed by the Act though individual states are now starting to introduce their own legislation to address this.

The Scheme now mandates that any 'organisation' (as defined above) must inform the OAIC and affected parties of a data breach (even if only "suspected") affecting them where "serious harm" is likely to occur. "Serious harm" may include serious physical, psychological, identity theft, and financial or reputation harm.

Other than the obvious financial penalties, breaches of the Australian Privacy Principles can have the following additional consequences:

- Loss of reputation and customer trust
- Harm to your customers and consequential litigation
- Reduced business functions and activities
- Loss of future income
- Failure to meet cyber insurance requirements to exercise compensation and remediation

Personal information is defined in s 6(1) of the Privacy Act as:

> "Information or opinion about an identified individual, or an individual who is reasonably identifiable, whether or not true and whether or not in material form".

However, the types of information that are personal information are unlimited and can vary widely as it is not limited to information about an individual's private or family life, but extends to any information or opinion that is about the individual, from which they are reasonably identifiable. This can include information about an individual's business or work activities.

The Act also gives rise to Australian Privacy Principals (APPs), legally binding principles forming the cornerstone of the privacy protection framework. The APPs set out standards, rights and obligations in relation to handling, holding, accessing and correcting personal information. The APPs provide the flexibility to tailor personal information handling practices to your needs and business model.

The APPs are structured to reflect the personal information lifecycle. They are grouped into five parts:

PART 1
Consideration of personal information privacy (APPs 1 and 2)

PART 2
Collection of personal information (APPs 3, 4 and 5)

PART 3
Dealing with personal information (APPs 6, 7, 8 and 9)

PART 4
Integrity of personal information (APPs 10 and 11)

PART 5
Access to, and correction of, personal information (APPs 12 and 13)

Breaches of the Australian Privacy Principles (APPs) are investigated by the Office of the Australian Information Commissioner (OAIC). The OAIC will refer to the 'Guide to Securing Personal Information, June, 2018' when assessing an entity's compliance with its IT security obligations in the Privacy Act. As such, it makes a lot of sense for organisations that are covered by the Privacy Act and subsequently the Scheme to be aware of these obligations and understand whether or not they currently comply.

We will now document some salient points from the Guide and highlight briefly how organisations can work towards implementing what the Guide states.

Good privacy practice is important for more than just ensuring compliance with the requirements of the Privacy Act. If an entity mishandles the Personal Information of its clients or customers, it can cause a loss of trust and considerable harm to the entity's reputation. Additionally, if Personal Information that is essential to an entity's activities is lost or altered, it can have a serious impact on the entity's capacity to perform its functions or activities.

It is important for entities to integrate privacy into their risk management strategies. Robust information-handling policies, including a privacy policy and data-breach response plan, can assist an entity to embed good information handling practices and to respond effectively in the event that Personal Information is misused, lost or accessed, used, modified or disclosed without authorisation.

Entities that handle Personal Information should build privacy into their processes, systems, products and initiatives at the design stage. Privacy should be incorporated into your business planning, staff training, priorities, project objectives and design processes, in line with APP1. Building privacy into data handling practices from the start, rather than 'bolting it on' at a later stage is known as 'privacy by design'.

The 'privacy by design' stage should also address Personal Information security, including the appropriateness of technology and the incorporation of information security measures that are able to evolve to support the changing technology landscape over time.

Entities should design their information security measures with the aim to:

- Prevent the misuse, loss or inappropriate accessing, modification or disclosure of Personal Information
- Detect privacy breaches promptly
- Be ready to respond to potential privacy breaches in a timely and appropriate manner

One way to achieve privacy by design is to conduct a **Privacy Impact Assessment** (PIA). A PIA is a written assessment that examines the privacy impacts of a project and assists in identifying ways to minimise those impacts. A PIA will assist in identifying where there are privacy risks, and where additional privacy protections may be required. Generally, a PIA should:

- Describe how personal information flows in a project
- Analyse the possible privacy impacts of those flows
- Assess the impact the project as a whole may have on the privacy of individuals
- Explain how those impacts will be eliminated or minimised

A detailed Guide to conducting PIAs is available from the OAIC website at Guide to undertaking privacy impact assessments — OAIC.

You may also need to conduct an **information security risk assessment** in conjunction with a PIA. An information security risk assessment is generally more specific than a PIA because it involves the identification and evaluation of security risks, including threats and vulnerabilities, and the potential impacts of these risks to information (including personal information) handled by an entity. As with a PIA, an information security risk assessment can be seen as an iterative process and may be undertaken across your business generally.

The findings of a PIA and information security risk assessment should inform the development of your risk management and information security policies, plans and procedures.

Once the risks have been identified, you should then review your information security controls (virtual and physical) to determine if they are adequate in mitigating the risks. Given that processes, information, personnel, applications and infrastructure change regularly, and given the constantly evolving technology and security risk landscape, regular review and monitoring of personal information security controls is crucial.

The Guide to Securing Personal Information, June, 2018 is a great tool to perform an information security risk assessment. The Guide introduces the concept of 'reasonable steps' that need to be taken protect Personal Information.

RSM

The reasonable steps will always depend on the circumstances, including the following:

- The nature of your entity
- The amount and sensitivity of the personal information held
- The possible adverse consequences for an individual in the case of a breach
- The practical implications of implementing the security measure, including the time and cost involved
- Whether a security measure is itself privacy invasive

The steps and strategies which may be reasonable to take according to the Guide are noted below. In order to protect any Personal Information that you hold, you essentially have to implement the steps and strategies mentioned below in your organisation:

- **Governance, culture and training**
  - Fostering a privacy and security aware culture
  - Oversight, accountability and decision-making
  - Personnel security and training.
- **Internal practices, procedures and systems**
- **ICT security**
  - Software security
  - Encryption
  - Network Security
  - Whitelisting and blacklisting
  - Testing
  - Backing Up
  - Email security
- **Access security**
  - Trusted insider risk
  - Identity management and authentication
  - Access to non-public content on web servers
  - Passwords and passphrases
  - Collaboration
  - Audit logs, audit trails and monitoring access
  - Individuals accessing and correcting their own personal information
- **Third party providers (including cloud computing)**
  - General issues
  - Cloud computing
- **Data breaches**
- **Physical security**
- **Destruction and de-identification**
  - Destroying personal information — irretrievable destruction
  - Destroying personal information held in electronic form — putting beyond use
  - De-identifying personal information.
- **Standards**

The list above can look at little overwhelming, but a methodical and detailed approach will get you there. Start with a health check to see how you stack up against the Guide. The key here is to recognise that this as a program of works and applying the relevant disciplines to it, as well as making available the necessary resources to complete the tasks is critical to success. This is not an activity that can be completed as a side project. Please also note that outsourcing the processing, transmission or storage (such as in the cloud) of Personal Information **does not** absolve the organisation collecting the data of its obligations to protect it.

If an organisation holds Personal Information of European citizens currently resident in the EU, you will also have significant international obligations under the *EU General Data Protection Regulation* which holds even more serious ramifications. Refer General Data Protection Regulation (GDPR) Compliance Guidelines

So please get on top of your Personal Information protection measures! The legislation came into force on 22 February, 2018 and if you haven't done so, you must act NOW!