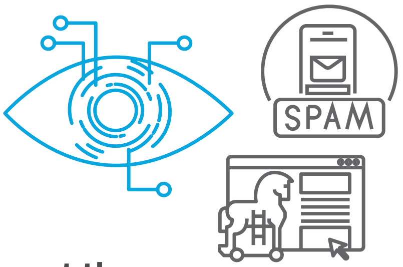
RISK ADVISORY SERVICES

– A Crash Course in Data Privacy and the Australian Privacy Principles (APPs)



Australia has seen many prominent cyber security breaches in recent times. Unfortunately, for every breach that is reported in the media, there are at least ten that go unreported.

We have seen literally millions of records being stolen as a result of some of the prominent data breaches that we have seen of late. A lot of these records either include Personally Identifiable Information (PII) or Personal Health Information (PHI). These end up in the dark web for sale which can later be purchased by other hackers for the purposes of identity theft which they then use for their own nefarious purposes. A complete medical record for an individual can fetch up to a thousand times more in the dark web then a single credit card number. The reason for this is very simple. A breached credit card will generally get cancelled within a matter of days rendering it useless. However, PII or PHI can be used to apply for three credit cards and two mortgages, as an example, providing the cybercriminal access to a much larger pool of funds.

The result of this privacy invasion can be devastating on the impacted individual. In some cases, it can take many months for an individual to get their identity back. During this time, they've struggled to obtain basic things like credit cards, mortgage, even access to basic utilities due to their poor or bad credit record. One of the key issues behind such large data losses is the fact that organisations hold on to personal information indefinitely. Not only is this in direct contravention of the APPs, this needlessly exposes a vast amount of data to potential breaches as we have seen already.

The above clearly highlights the devastation that can be caused but the loss of an individual's personal information. As a result of this, it is critical to protect an individuals' personal information. The key pillar to this in Australia are the Australian Privacy Principles (APPs). This article will explore some of the key aspects of the APPs, the organisations that are in scope, the important link between data privacy and data security, the concept of privacy by design and steps to auditing data privacy.

Definition of Data Privacy

- Data Privacy is a part of the data protection area that deals with the proper handling of data focusing on compliance with data protection regulations
- Data Privacy is centered around how data should be collected, stored, managed, and shared with any third parties, as well as compliance with the applicable privacy laws (such as Australian Privacy Principles (APPs) or General Data Protection Regulation (GDPR))
- The focus generally is personal information – "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" — APPs.

What are the Australian Privacy Principles (APPs)

- The Australian Privacy Principles (or APPs) are the cornerstone of the privacy protection framework in the Privacy Act 1988 (Privacy Act). They apply to any organisation or agency the Privacy Act covers
- There are 13 Australian Privacy Principles and they govern standards, rights and obligations around:
  - The collection, use and disclosure of personal information
  - An organisation or agency's governance and accountability
  - Integrity and correction of personal information
  - The rights of individuals to access their personal information
- The Australian Privacy Principles are principles-based law. This gives an organisation or agency flexibility to tailor their personal information handling practices to their business models and the diverse needs of individuals. They are also technology neutral, which allows them to adapt to changing technologies.
- A breach of an Australian Privacy Principle is an 'interference with the privacy of an individual' and can lead to regulatory action and penalties.
- 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).

Organisations in Scope

- 'APP Entities' are defined as 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). Please note that any organisation handling Personal Health Information is in scope regardless of turnover.
- State Government agencies are not generally governed by the Act though individual states are now starting to introduce their own legislation to address this.

Consequences of a Privacy Breach

The consequences of a privacy breach can vary and include the following:

- Fines and penalties
- Loss of reputation and customer trust
- Harm to your customers and consequential litigation
- Reduced business functions and activitiesLoss of future income and/or
- Failure to meet cyber insurance requirements to exercise compensation and remediation.

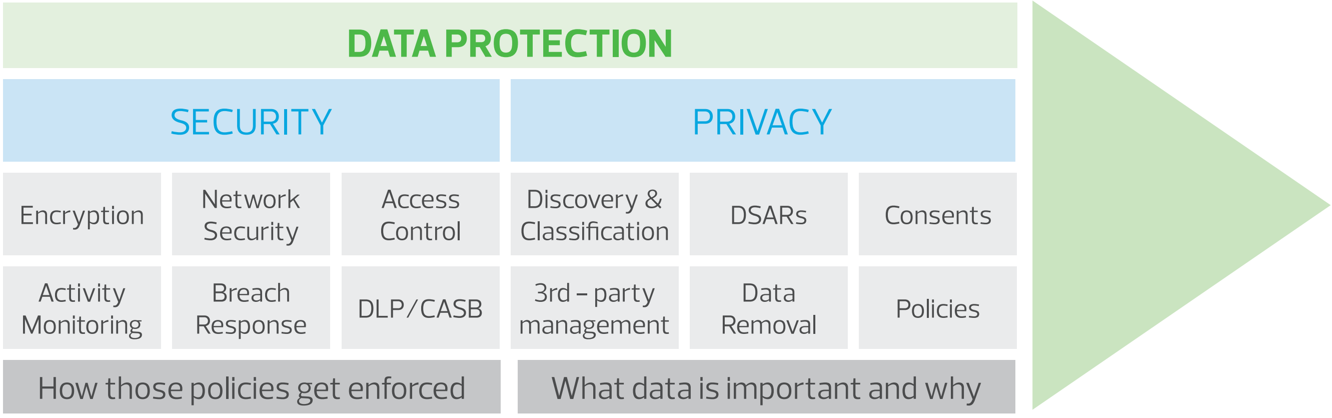
The Link Between Data Privacy and Data Security

Data Privacy Definition

- Data Privacy focuses on the rights of individuals, the purpose of data collection and processing, privacy preferences, and the way organisations govern personal data of data subjects.
- It focuses on how to collect, process, share, archive, and delete the data in accordance with the law.

Data Security Definition

- Data Security includes a set of standards and different safeguards and measures that an organisation is taking in order to prevent any third party from unauthorised access to digital data, or any intentional or unintentional alteration, deletion or disclosure of data.
- It focuses on the protection of data from malicious attacks and prevents the exploitation of stolen data (data breach or cyber-attack). It includes Access control, Encryption, Network security, etc.
- Data security can help achieve data privacy objectives by safeguarding personal information. This linkage is best visualised as noted below:



DATA PROTECTION					
SECURITY			PRIVACY		
Encryption	Network Security	Access Control	Discovery & Classification	DSARs	Consents
Activity Monitoring	Breach Response	DLP/CASB	3rd – party management	Data Removal	Policies
How those policies get enforced			What data is important and why		

Principle of 'Privacy by Design'

- 'Privacy by design' principles are critical in ensuring that processes, systems, products and initiatives protect personal information from the start. The principles include the following key elements:
- Build privacy into your processes, systems, products and initiatives at the design stage
- 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.

The OAIC's "The Guide to Securing Personal Information, June, 2018"

The Guide to Securing Personal Information, June, 2018 is a tool to perform an information security risk assessment. The Guide can be useful in understanding and bolstering data security mechanisms that will allow the protection of personal information.

- The Guide introduces the concept of 'reasonable steps' that need to be taken protect Personal Information
- Areas covered:
  - Governance, culture and training
  - Internal practices, procedures and systems
  - ICT security
  - Access security
  - Third party providers (including cloud computing)
  - Data breaches
  - Physical security
  - Destruction and de-identification
  - Standards.

The ISO 27701 Standard

ISO/IEC 27701: Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines is also a key guideline that can be used to implement privacy related controls within an organisation. It can be used in conjunction with the OAIC's guide to provide a comprehensive framework to managing and protecting personal information within an organisation. However, care should be taken on not doubling up on controls in order to focus efforts on key controls needed to protect personal information.

Steps to Auditing Data Privacy

With the devastation that can be caused by the loss and illicit sale of personal information, it is important to protect personal information as outlined above and also to exercise due diligence over these controls to ensure that they are operating effectively. This is where an effective audit function is critical. Outlined below are some key steps to auditing data privacy:

- Perform a desktop review of all relevant policies and procedures assessing alignment with ISO/IEC 27701:2019 Privacy Information Management System controls
- Assess the privacy risk management processes in line with privacy risk management capabilities and management of Personally Identifiable Information (PII) and/or Personal Health Information (PHI)
- Arrange discussions with key personnel within the relevant service areas to gain an understanding of controls for managing data privacy, including information classification and handling practices and records management policy
- Perform walkthroughs to gain an understanding as to how data is managed (particularly for PII) and whether this is consistently applied
- Review the controls and procedures in place that impact information privacy and confirm that they are aligned to the control objectives outlined in ISO/IEC 27701's Annex A and/or Annex B controls
- Ascertain the content and effectiveness of the privacy awareness program for staff and the effectiveness of existing communication channels
- Ascertain processes in place for reporting of privacy risks and/or data breaches
- Integrate privacy into their risk management strategies
- Robust information-handling policies, including a privacy policy and data-breach response plan.

Data privacy is centred around management and protection of personal data. The APPs are the guiding principles in Australia with 13 prescribed principles. Most organisations in Australia are in scope for the APPs. There is a strong linkage between data privacy and data security with data security focused on the protection of data including PII and PHI. Principles of 'privacy by design' and the 'The Guide to Securing Personal Information, June, 2018' are key to designing secure systems and protecting the data they handle. Additional guidance on privacy data management can be obtained from the ISO/IEC 27701:2019 Privacy Information Management System standards. Privacy audits are a key way to ensure organisational compliance. With the devastation that can be caused by the loss and misuse of personal information it is critical to protect this information as outlined in this paper.

For more information please contact:

Ashwin Pal
Partner, Sydney
T 02 8226 4500
E ashwin.pal@rsm.com.au

Darren Booth
Partner, Melbourne
T 03 9286 8158
E darren.booth@rsm.com.au

Riaan Bronkhorst
Principal, Perth
T 08 9261 9272
E riaan.bronkhorst@rsm.com.au