protiviti
Global Business Consulting

Managing Privacy Under One Roof

Introduction

Australia has just kicked off its Privacy Awareness Week (PAW) led by the Office of the Australian Information Commissioner (OAIC). PAW 2022 will be held from 2 – 8 May.

With regulatory change on the horizon with the Attorney-General's Department currently reviewing the Privacy Act 1988 and proposing reform[1], high volumes of unrestricted personal data or misuse of personal data by external parties regularly reported in the media, and organisations continuously increasing their data footprint and exploring new ways of using personal information, 2022 will be a landmark year in the Australian privacy landscape

This year's PAW theme is *Privacy: The Foundation of Trust* and will explore the building blocks and foundations organisations can put in place to secure personal information. At Protiviti, we believe the cornerstone of a responsible, secure, and compliant privacy program is implementing and maintaining a privacy framework.

Privacy pain points and challenges

The annual 'Executive Perspectives on Top Risks'[2], a joint survey conducted by Protiviti and NC State University's ERM Initiative highlighted that privacy and information security continue to be a heavy burden on Executives' minds. Based on our experience working with organisations of all sizes, across various sectors, we observe consistent themes and pain points in relation to data privacy and security, with key highlights noted below:

- **Poor visibility over personal data repositories** – Despite the increased risk exposure, most organisations continue to collect, process, store and transmit large volumes of personal data in an informal manner. Mountains of personal data sitting inside and outside structured data repositories (e.g. systems, databases) and poorly designed retention policies lead to significant compliance and operational problems which continue to be brushed aside by even the mature organisations. Increased use of cloud platforms and remote working practices have also further exacerbated this matter.
- **Inadequate security controls over personal data** – Some organisations continue to struggle to embed strong access controls (e.g. user authentication and authorisation, user re-certification, encryption) to safeguard personal data repositories and the underlying infrastructure. Existence of legacy systems that are incapable of single-sign-on ('SSO') and poorly managed endpoint or Bring Your Own Device ('BYOD') policies are some common technology challenges that make governing data processing IT assets a nightmare for IT security staff. Financial constraints and other business priorities also mean that organisations hesitate to invest in identity and access management or data loss prevention solutions and continue to use manual and labour-intensive processes (e.g. spreadsheet-based user access reviews).

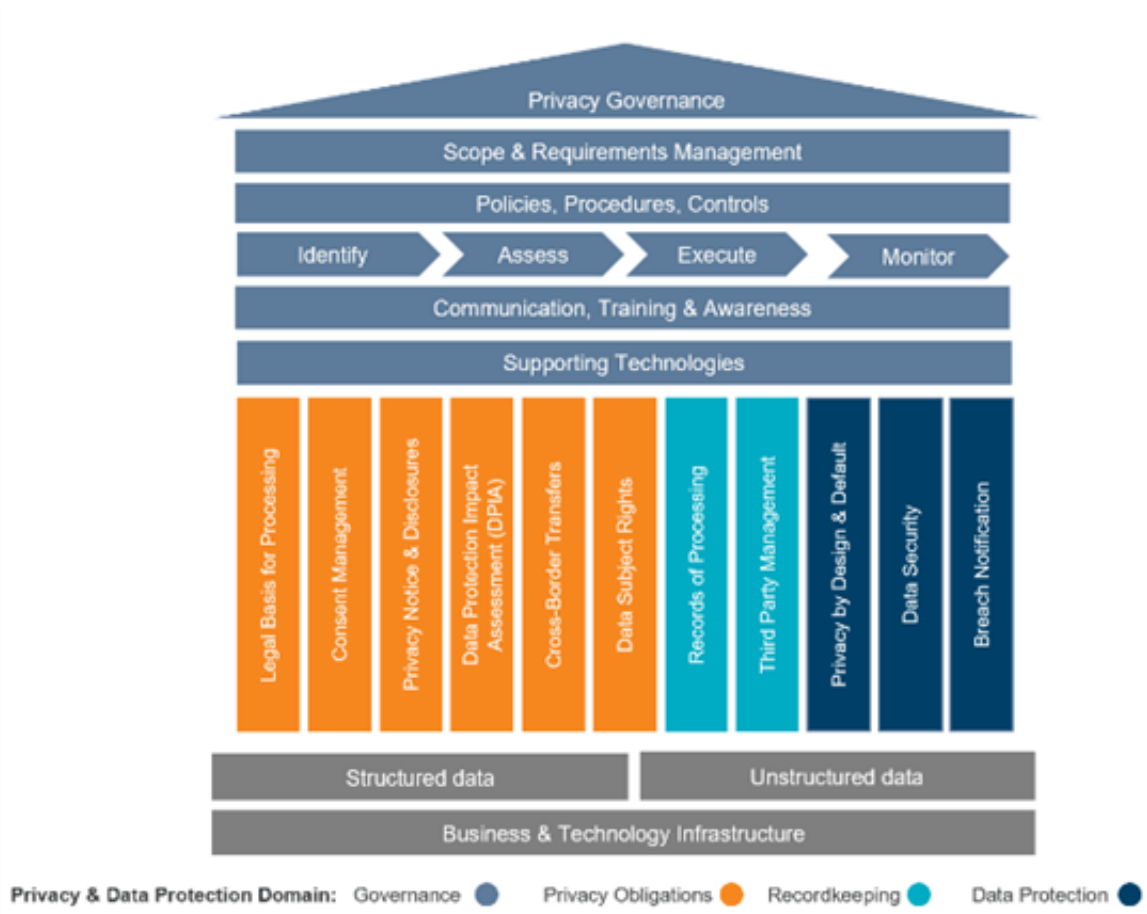
- **Limited oversight over data processors -** Cost cutting measures and an abundance of cloud service providers (e.g. Software-as-a-Service, Infrastructure-as-a-Service, Platform-as-a-Service) have led organisations to outsource their business and support functions. As a result, increased number of vendors, business partners and other third parties have access to a firm's precious personal information (not to mention sensitive business data). However, to tackle this heightened risk organisations do not consistently apply strong vendor due diligence methods, robust data processing agreements, or vendor monitoring and assurance procedures to reduce the risk of misuse or mishandling of personal data by external parties. This is exacerbated by 'shadow IT' where end users purchase their own cloud solutions, often on a credit card.
- **Complex privacy regulatory landscape:** Many global organisations have to comply with multiple regulators and/or regulations (for example, think about an Australian software company that sells its product in multiple countries, including the European Union; or a bank with customers and/or employees in many countries) that may at times conflict or contradict one another. Maintaining compliance and staying on top of changes to requirements can be a challenging task. Inability to clearly grasp different privacy obligations and requirements could also possibly lead to hefty fines and supervisory enforcement actions.

Seeing the bigger picture

With increasing regulatory demands and various elements of data privacy (e.g. policy and procedures, data breach processes, privacy assessments, data retention and security), we find that organisations do not have a methodical and consistent approach to managing privacy requirements across the organisation. Especially, if you have many business functions and areas that collect, process and manage personal data (e.g. Human Resources, Payroll, Marketing, Sales, Customer Services, etc.).

As privacy practitioners, we continue to emphasise the importance of having a framework to address data privacy requirements and regulations, as this not only ensures that organisations are taking necessary precautions to protect personal data but it encourages strong data governance.

Our experience in running privacy programs indicate that if you are dealing with large volumes and/or high risk (e.g. patient and health records) personal data, it is highly beneficial to have a privacy framework or operating model that sets out clear privacy compliance requirements and control areas. Highlighted below is Protiviti's Privacy Management Framework which outlines the core building blocks to managing privacy:



- **Governance**: Sets out the tone-at-the top from the senior leadership around guiding principles and direction for privacy and data protection. Governance and accountability are critical elements to get right, as these shape the way a privacy program is built, operated and embraced throughout the organisation.
- **Privacy Obligations**: In order to effectively meet privacy obligations, it is important to build a baseline and scope of regulatory obligations (e.g. legal basis, consent, disclosures, cross-border transfers) and monitor changes to these. In the absence of this clear view, organisations will always be playing catch-up in a complex regulatory environment.
- **Recordkeeping:** Maintaining accurate, relevant and complete records of personal data is a common set of expectations or requirements across different privacy regulations e.g. GDPR Article 30, APP 10, CCPA 999.317). Building and maintaining an inventory of data processing activities and vendors would be a good step in the direction as this will enable better transparency over where personal data comes from, where it sits, who has access to it, and what vendors deal with it, etc.
- **Data Protection**: there are countless stories of human error or lack of security leading to major data and privacy breaches, and even the most well organised companies are vulnerable to this at any point in time. Putting in necessary safeguards and control measures to protect personal data is imperative in avoiding data losses, breaches, regulatory fines and ultimately reputational damage to a company.

  Personal data tend to sit either across organised data repositories such as relational databases or platforms (i.e. structured data) or as various file formats (e.g. text files, images,

spreadsheets) that are scattered across file shares and directories (i.e. unstructured data).

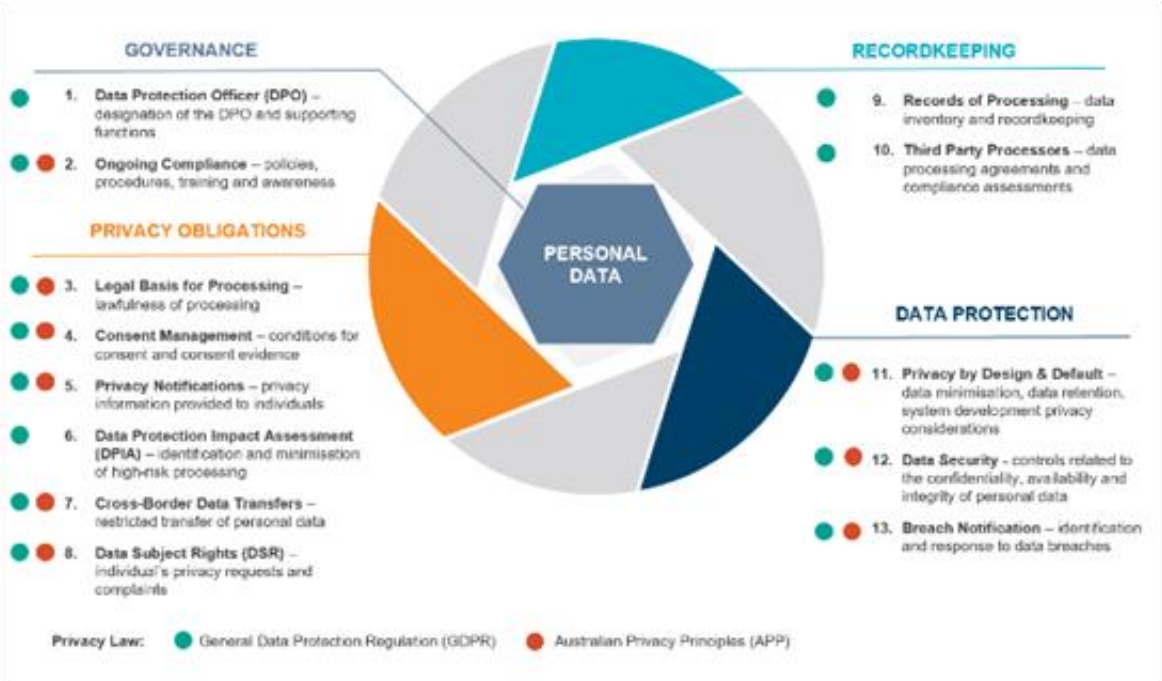
Business and technology infrastructure provide the foundations where personal data assets are stored and processed.

A privacy framework can provide the foundation to build a privacy function as well as identify gaps and weaknesses within privacy practices, and then develop appropriate action plans or roadmaps to achieve, maintain and validate compliance. It also puts privacy (which can be a complex subject) into a digestible format to better inform the senior leadership and other key stakeholders.

We also recognise that an effective privacy framework should be flexible enough to accommodate different regulatory frameworks and guidelines. To illustrate this point, we have mapped Protiviti's Privacy Management Framework against the GDPR and Australian Privacy Principles ('APP') to provide a reference point on how these two distinct regulations stack up against the framework.

In a highly digitised and globalised world where data is considered to be the new oil, organisations will continue to accumulate mass wealth of personal data that can add to administrative and compliance burdens. However, having a cohesive top-down framework that sets out different privacy domains and risk areas can help a firm set out its privacy policies, procedures and protocols across the enterprise, especially for one that faces disparate (and sometime conflicting) privacy regulations and rules. A privacy framework also helps organisations assess and remediate privacy gaps and implement changes to achieve and maintain compliance in a more sustainable way.

Protiviti's subject matter experts continue to support and provide guidance around privacy and security related challenges. To learn more about Protiviti's services relating to privacy, please visit our website.



Contacts

Ewen Ferguson
+61.478.491.056
ewen.ferguson@protiviti.com.au

Hirun Tantirigama
+61.423.853.453
hirun.tantirigama@protiviti.com.au

Marc Coleman
+61.405.189.472
marc.coleman@protiviti.com.au

protiviti®