DATA PROTECTION WHITE PAPER

COMPLYING WITH SAAS DATA MANAGEMENT PRINCIPLES: AUSTRALIA AND NEW ZEALAND

SPANNING

CONTENTS

INTRODUCTION

The rapid adoption of cloud and SaaS technologies around the globe is mirrored in the adoption of those technologies in Australia, bringing issues to the fore regarding data protection, data ownership, data privacy, and data sovereignty. The proliferation of SaaS solutions, and SaaS data in particular, are now the focus of much legal, political, and corporate discussion, resulting in the creation of new policies and compliance standards for SaaS data management.

What are the key considerations and primary regulatory issues that organisations must consider as they prepare to adopt services such as Microsoft Office 365? How does IT help ensure that not only their organisation, but their SaaS application vendors, are compliant with data sovereignty regulations?

IN THIS REPORT, YOU WILL LEARN:

- The current state of cloud and SaaS adoption in Australia.
- What the evolution of, and disintermediation of, IT from on-premise to SaaS means for those concerned with compliance for SaaS data.
- Some ramifications of data sovereignty and data residency requirements that are critical for those adopting SaaS and cloud technologies.
- How to assess risks from potential gaps in SaaS providers' services and security.
- What to do now—including a "SaaS Provider Checklist" for Australian IT organisations who are vetting SaaS vendors.

THE STATE OF CLOUD AND SAAS ADOPTION IN AUSTRALIA

Cloud adoption in Australia continues to grow at a rapid pace. The total public cloud infrastructure services market (PaaS and IaaS) is projected to increase nearly 112% from 2015 through 2019, according to the Telsyte Australian Infrastructure & Cloud Computing Market Study 2015. The total market value for public cloud infrastructure services is expected to reach $775 million by 2019. In addition, Telsyte research shows Software as a Service (SaaS) penetration ranges from 19 percent to 63 percent across 25 different categories of enterprise software measured.

Analysts reporting on the broader Asia-Pacific (AP) region show similar growth, with the most rapid growth coming from SaaS technologies at a projected growth rate of 22.5%. Sid Nag, research director at Gartner, states "The public cloud market continues to grow in the mature AP market with SaaS as the primary growth segment. Organisations are pursuing a cloud first strategy focused on migrating software applications to the cloud driving this growth."

In short, if you work in IT in Australia and New Zealand, cloud and SaaS technologies are likely to become a larger part of your future.

"The public cloud market continues to grow in the mature AP market with SaaS as the primary growth segment. Organisations are pursuing a cloud first strategy focused on migrating software applications to the cloud driving this growth."

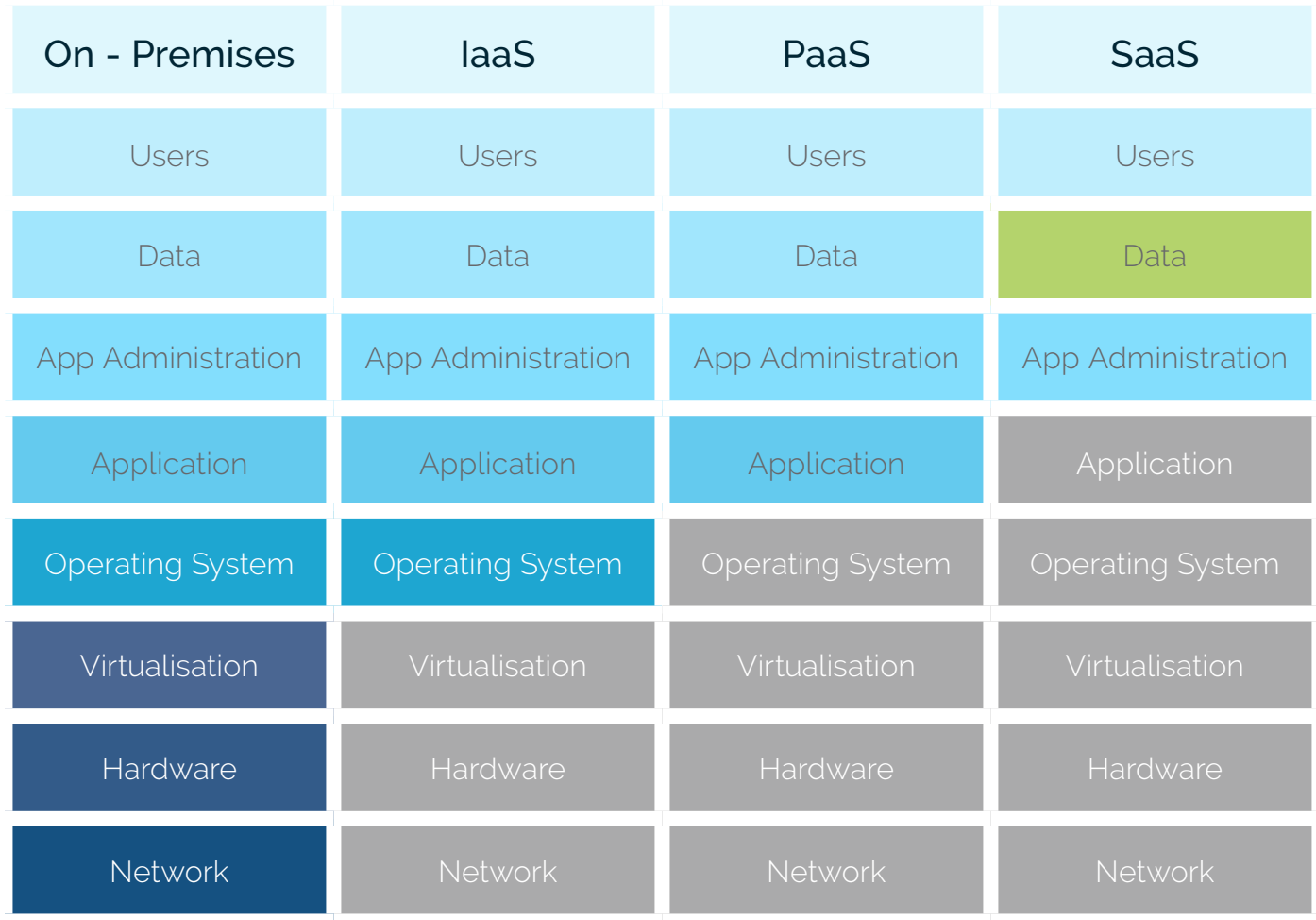
Sid Nag
RESEARCH DIRECTOR, GARTNER [1]

[1] http://www.gartner.com/newsroom/id/3360517

THE EVOLVING RESPONSIBILITY OF IT REGARDING SAAS DATA

Although cloud and SaaS adoption is trending upward, in part due to anticipated cost and labor savings; adopting these technologies does not lessen IT's ownership or responsibility regarding data protection, as illustrated in the diagram below.

Before the advent of cloud computing and SaaS applications, IT was responsible for managing all components of the stack. With a SaaS application, IT no longer owns the app, but still owns the app data, and is responsible for protecting that data.



IT Deployment Models and Data Management Responsibilities

When the IT deployment model is completely **on-premises,** IT is responsible for everything, including planning, architecting, deploying, managing, and protecting the physical components, the software, the application administration, the data, and the users.

When the IT deployment model is **Infrastructure as a Service (IaaS),** the IT vendor will manage the network hardware, and the virtual machines. IT is still responsible for managing the operating systems on the VMs, deploying and managing the operating system that is on the VMs, as well as the applications. In addition, IT is still responsible for management of the data and the users.

With **Platform as a Service (PaaS),** the service provider not only manages all of the hardware required, but they also manage the operating systems on the virtual machines. IT is responsible for installing and managing the applications, the data, and of course the users.

With **Software as a Service (SaaS),** the service provider manages all of the hardware and software. IT only manages the administration of the application (via policies provided by the service provider) and the users. Data management is a shared responsibility.

Regardless of which model of service delivery is in place within an organisation, IT is responsible for ensuring data management aligns with regulatory requirements, organisational governance, and defined controls. Ultimately IT must also meet the organisation's need for business continuity.

REGULATORY REQUIREMENTS AND KEY DEFINITIONS

For global customers moving to SaaS and cloud apps, it is important that both vendors and customers research data privacy laws for their region. For the scope of this report, we will cover the Australian Privacy Principles (APPs).

Data sovereignty is "the concept that information which has been converted and stored in binary digital form is subject to the laws of the country in which it is located." Further, the term refers not just to laws limiting cross-border data transfer, it also encompasses the need to comply with foreign legal requirements for data handling and data residency. Similar to data sovereignty, data residency refers to the legal or regulatory requirements imposed on data, based on the country or region in which the data resides.

The **Australian Privacy Principles (APP)** provide guidance for the evolving responsibilities of today's IT departments, and are particularly important when considering SaaS and cloud data. While the information that follows is not a substitute for your own organisation's legal team and their guidance, there are certain requirements that must be met by SaaS and cloud providers—and your organisation—to comply with Australian law, and to keep in compliance.

What are the Australian Privacy Principles (APPs), and which APPs are most relevant for those using SaaS and cloud services?

In March 2014, 13 Australian Privacy Principles (APPs) replaced the National Privacy Principles (NPPs). The APP guidelines outline the mandatory requirements of the APPs, and how the Office of the Australian Information Commissioner (OAIC) will interpret the APPs.

APPs contain information regarding rules for managing digital data, and for meeting data sovereignty requirements. For a complete list of all APPs, see the Office of the Australian Information Commissioner here.

Abridged APP definitions for the 13 APPs most relevant for those evaluating SaaS solutions follow in the table on the next page.

AUSTRALIAN PRIVACY PRINCIPLES

The following are the seven APPs most relevant for those using SaaS and cloud services.

APP 1 MANAGEMENT OF PERSONAL INFORMATION

Requires organisations to have ongoing practices and policies in place to ensure that they manage personal information in an open and transparent way. Organisations must take reasonable steps to implement Security and Compliance practices that include documentation of policy and procedures for:

- Details of what data they collect, process, and store;
- How the data is collected;
- How the data is used;
- Whether or not the data is likely to be transferred out of the country;
- Requirements to allow individuals the ability to access their data for updates and changes.

APP 3 DATA COLLECTION

This requirement is specific to the lawful and and fair collection of personal data, ensuring the Entity has a reasonable requirement to collect it and that consent from the individual has been established.

APP 4 DATA COLLECTION - UNSOLICITED

If an entity receives personal information that it has not solicited from an individual, it must first determine whether or not it could have collected the information under APP 3 if it had solicited the information. If not, it must destroy or de-identify the information.

APP 5 NOTIFICATION OF THE COLLECTION OF PERSONAL INFORMATION

Requires organisations to notify individuals about the access, correction, and complaints processes in their APP privacy policies, and also the location of any likely overseas recipients of individuals' information.

APP 6 DATA USE AND DISCLOSURE

Referring to an organisation's use and disclosure of personal information, it provides that, as a general rule, an organisation should only use or disclose personal information for the purpose for which it was collected.

APP 7 DIRECT MARKETING

Defines circumstances in which an organisation can use personal information for direct marketing, and prohibits private sector organisations from using personal information for direct marketing except in certain limited circumstances.

APP 8 CROSS BORDER DISCLOSURE

This requirement covers the disclosure of personal information outside of Australia. It is particularly relevant in a context where an increasing number of entities use information technology services that disclose or transfer personal information to overseas recipients (such as outsourcing, off-shoring and cloud computing). Subject to certain exceptions, before an organisation makes personal information available to a third party located outside of Australia, the organisation must take reasonable steps to ensure that the overseas recipient does not breach the APPs. This will usually involve the APP entity entering into an enforceable contractual arrangement with the overseas recipient that requires the recipient to handle the personal information in accordance with the APPs.

There are additional requirements regarding the management of SaaS and cloud data, such as security and location of data while in transit and at rest, strong encryption, and intrusion detection, which will be discussed in the next section.

ADDRESS THE GAPS

At a high level, the adoption of SaaS and cloud technologies does not remove the responsibility for data protection from IT; the shift may, however, obscure areas of risk. SaaS and cloud vendors are generally secure, and generally protect customer organisations from their own infrastructure failures. They cannot, however, protect organisations from human (administrator and user) error, programmatic (sync and integration) errors, or malicious activity.

For example, Microsoft notes that, **"With Microsoft, you are the owner of your customer data.** Microsoft will use your customer data only to provide the services we have agreed upon, and for purposes that are compatible with providing those services." They will delete data you've instructed them to delete—even if the deletion is in error, or an accidental programmatic overwrite.

> "With Microsoft, you are the owner of your customer data. Microsoft will use your customer data only to provide the services we have agreed upon, and for purposes that are compatible with providing those services."

The globalisation of data workloads and the global reach of many SaaS providers introduce new compliance risks for Australian IT departments, especially concerning APP 1 (Management of Personal Information) and APP 8 (Cross Border Disclosure). SaaS and cloud data can be transferred across regional barriers to data centers across the world. That is why you must verify that your SaaS or cloud vendors adhere to APP 8, and agree to keep data in transit within the boundaries of the region. Legal obligations to the treatment of cloud data vary from country to country across the world.

WHEN EVALUATING SAAS AND CLOUD VENDORS, IT SHOULD:

- **Review** the vendor's posted security and privacy policies, and prepare questions if details on how they would handle your organisation's data are not readily available
- **Understand** where the vendor's data centres are located, which data centre would house your organisation's data, and if the vendor aligns with the relevant Australian Privacy Principles as listed above and here.
- **Obtain** documentation from the vendor detailing what should be multiple layers of operational and physical security to ensure the integrity and safety of their customers' data. These security protocols will be listed specifically in the SaaS Provider Checklist.

NEXT STEPS IN CHOOSING A SAAS DATA PROTECTION VENDOR

SAAS PROVIDER CHECKLIST *When evaluating whether your SaaS and cloud vendors have the controls in place sufficient to meet APP and other regulatory requirements, the checklist below will help you start the conversation with potential SaaS vendors.*	ANSWER
Does the SaaS vendor have a formal Security and Compliance program to ensure data protection for all data collected, stored or otherwise processed through their service?	
Does the vendor only collect data from those who have given their consent by accepting the vendor's terms of service?	
If an organisation receives personal information that it has not solicited from an individual, will it collect only the data of customers who subscribe to their service?	
Are details related to notifications for the collection of data covered in the vendor's Privacy Program, and are these details available on the vendor's website or via documentation provided by the vendor?	
Does the vendor disclose the data residence for data collected, and does that residence meet data sovereignty and compliance regulations?	
Has the vendor successfully completed the SSAE 16 SOC 2 audit certification process, a rigorous evaluation of repeatable operational and technical controls?	
Does the vendor protect data at rest with 256-bit AES object-level encryption—one of the strongest block ciphers available?	
Does the vendor protect all data in transit with Secure Socket Layer (SSL) encryption?	
Does the vendor use systematic intrusion detection, including log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting, and active response?	
Does the vendor compartmentalize and limit access to the production environment, only granting access to named employees who have specific operational requirements?	
Are changes to the vendor's production environment access control list tracked and auditable?	
If the vendor uses third party services, are those services ISO 27001 certified, have they completed multiple SAS-70 Type II audits, and do they publish a SOC 2 report under both the SSAE 16 and the ISAE 3402 professional standards?	
Is the vendor certified under the US-EU Privacy Shield?	

SAAS DATA PROTECTION AND BUSINESS CONTINUITY

It's important to understand and ensure that your organisation complies with regulations and controls regarding SaaS data. Beyond regulations and policies, IT needs to plan to ensure SaaS data is safe, backed up, and quickly restorable for business continuity needs.

If your organisation has adopted, or is considering adopting, a SaaS productivity platform such as Microsoft Office 365, ensure you can protect against the common issues that can lead to SaaS data loss.

One best practice to meet those requirements is to adopt a backup-and-restore solution like Spanning Backup for Office 365.

Spanning Backup for Office 365 provides enterprise-class backup and restore for Office 365 data, developed to meet the fastest Recovery Time Objective (RTO) requirements for business continuity. Spanning backs up Office 365 Mail, Calendars, OneDrive for Business, and SharePoint Online data automatically, every day.

Spanning also supports customers making additional on-demand backups anytime, such as before making major changes to a production environment.

TOP 3 SAAS DATA LOSS ISSUES

01 **HUMAN ERROR**
Including misconfigurations, accidental deletions or overwrites, and administrative mistakes.

02 **PROGRAMMATIC ERRORS**
Such as sync errors, integration errors, and improperly tested customizations.

03 **MALICIOUS ACTIVITY**
Such as ransomware and other malware.

SAFEGUARD YOUR ORGANISATION

Metadata is included in the data that Spanning backs up daily, to enable fast recovery in the event of data loss. Spanning supports the rapid restoration of Mail, Calendars, OneDrive for Business, and SharePoint Online items to their full original state – including point-in-time snapshots of folder structure, categories, and more.

Spanning meets data residency requirements via its Sydney data centre, where ANZ data will reside; and **Spanning aligns with the Australian Privacy Principles as follows.**

- **APP 1:** Spanning has implemented a formal Security and Compliance program to ensure data protection for all data collected, stored or otherwise processed through our service.
- **APP 3:** Spanning only collects data from Entities who have consented through the acceptance of our terms of service.
- **APP 4:** Spanning collects only the data of our Customers who subscribe to our service.
- **APP 5, 6, and 7:** Details related to notifications for collection of data are covered in the Spanning Privacy Program and are available on the Spanning website.
- **APP 8:** Spanning has launched the Spanning Backup for Office 365 service in the Australian and New Zealand market. Data collected in Australia is stored in Australia.

For more information, go to http://spanning.com/products/office365-backup/. And to evaluate whether Spanning Backup for Office 365 is an appropriate solution for your organisation, contact us for a free 14-day trial or a demonstration of the solution.

Spanning Cloud Apps is the leading provider of backup and recovery for SaaS applications, protecting thousands of organizations from data loss due to user error, malicious activity and more. We are the only global provider of powerful, enterprise-class data protection for Microsoft Office 365, G Suite, and Salesforce. With data centers located in North America, the EU, and Australia, Spanning is the most trusted cloud-to-cloud backup provider with millions of users around the world.

Spanning Backup for Office 365

501 CONGRESS AVE, SUITE 200
AUSTIN, TEXAS 78701
P +1.512.236.1277

SPANNING.COM