THE IMPLICATIONS OF DATA SOVEREIGNTY IN AUSTRALIA AND ABROAD

Considerations for best practice in 2024

By Sarah Brichet, Simon Liu, Jacky Zeng, and Mike Trovato

November 2023

The Implications of Data Sovereignty in Australia and Abroad

Introduction

The digital economy has grown exponentially in the recent decade, and data has become one of the most important resources in the world. Data created, collected, or used in organisational processes no longer only serve as an enabler of products, but can be the product itself to serve billions of users worldwide [1].

Concurrently, the mainstream use of cloud service providers has enabled domestic organisations to have vast amounts of their data handled and stored offshore by a range of companies. The situation becomes even more complex for organisations collect and handle data containing personal information. Where such organisations operate internationally, the storage of personal information may not necessarily be in the same location as the individuals to whom it relates, leading to questions of which privacy laws in what jurisdiction(s) may apply.

Further, ensuring hosting arrangements address matters relating to data sovereignty, ownership structure, liability, supply chain and transparency arrangements (as well as requirements set by organisations to reduce risks pertaining to these matters) can be challenging and limit commercial opportunity.

In this context, it is necessary for any organisation to consider where their data is stored, risks associated with that data, who has access to it, the contractual obligations associated with data handling, what domestic and international laws can be asserted over it, and any relevant industry policies, standards, and procedures that they must demonstrate compliance with.

What is data sovereignty?

Data sovereignty refers to the jurisdictional control or legal authority that a State has to assert its rights or control over data because of its physical location of storage which is within their jurisdictional boundaries. The concept encompasses the notion of **data residency** – which refers to the physical location of where the data is stored.

Data sovereignty comes into play when domestic data moves across jurisdictional borders, including when it is stored within another country's or state's geography. The most common way this occurs is when an organisation uses a cloud service provider with data centres outside of their geography.

Questions of data sovereignty also arise in organisations that need to perform cross-border data transfers. Organisations that operate in different jurisdictions, and transfer and store their data across multiple jurisdictions, will need to be especially cognisant of the challenges to data sovereignty when operating in an international landscape, due to a high degree or variability in compliance requirements.

The Implications of Data Sovereignty in Australia and Abroad

Data sharing vs. data localisation vs. data access

Many countries and states have enacted data sovereignty laws governing certain types of personal or sensitive information, as well as data which may have national security implications.

Data sovereignty requirements can be broadly split between three types of rules:

- Rules that qualify how organisations may share and store domestic data offshore – **data sharing rules**
- Rules that require that certain data generated within a country's borders is stored within its borders – **data localisation**, and
- Rules that enable governments (or related departments and agencies) to access an organisation's data – **data access rules**.

Data sharing rules seek to understand and mitigate the risks of sharing and storing data offshore. **Data localisation rules** aim to eliminate that risk by ensuring that statutory protection is preserved. It helps to make sure that only one jurisdiction's laws apply and greatly reduces the exposure to adverse data sovereignty risks – e.g., unauthorised foreign access to an organisation's data. Lastly, **data access rules** permit the access of an organisation's data, often for national security or law enforcement reasons. Data access rules enabling 'lawful' access vary greatly between jurisdictions which make them an important data sovereignty consideration.

The application of these rules depends on the type and sensitivity of information an organisation handles, the type of activities an organisation conducts, and the sector an organisation operates in. Understanding the circumstances in which they apply to your organisation is an essential step of ensuring appropriate measures to manage data sovereignty.

Why is data sovereignty important?

Data sovereignty plays an important part in several domains [2]:

- **Regulatory:** Governments are increasingly cognisant of the protection of personal and organisational data, as well as maintaining control over data that may have national security implications. In Australia, several data sovereignty laws impose obligations on certain organisations depending on the type, sensitivity, and criticality of information they handle, the type of activity they conduct, and the sector they operate in. Organisations that transfer or store their data offshore or to other states may need to consider these factors in ensuring compliance with obligations under the law.

The Implications of Data Sovereignty in Australia and Abroad

- **Loss of control:** The act of hosting data offshore poses risks to how an organisation may exercise control over its data. Offshore cloud services are likely subject to the laws of other countries, where Nation States may exercise covert data collection without the organisation's knowledge and amend their privacy laws without the organisation's notice. Further, Australian-owned cloud service providers operating overseas may be subject to another government's access to the data they handle and store [3].

  Storing data with a cloud service provider introduces new threats and increases the risk for the data sent offshore to be accessed or interfered with by foreign actors. This may be a significant consideration for organisations who are concerned about data sovereignty risks.
- **Privacy:** Ensuring that personal information is adequately protected, including when shared or disclosed to overseas or other domestic jurisdictions, is required by privacy law federally and in most states and territories of Australia [4]. It is important for businesses transferring personal information overseas to take reasonable steps to ensure that the information will be handled in an appropriate and secure manner consistent with the Australian Privacy Principles (APPs) or the relevant state or territory counterpart.
- **Data security:** The Australian Signals Directorate (ASD), which is responsible for foreign signals intelligence, supports the increase in government and corporate regulations to improve data and system security, which will in turn position Australia as an attractive location for global and domestic businesses that handle personal or sensitive data.
- **Business continuity:** An organisation's ability to access to its data in the event of a disaster or disruption is essential to business continuity. If data is stored in a different country, there may be legal or technical challenges to accessing it in a timely manner. Some regulators, such as the Australian Prudential Regulatory Agency (APRA) have required certain organisations, such as major banks to demonstrate they can bring offshored operations back to Australia in a crisis situation.
- **Trust:** Considering the recent wave of data breaches, establishing and maintaining trust among clients and the public is a critical requirement for organisations conducting business. This is particularly important for entities entrusted with sensitive client data or those offering essential services. When it comes to data security, opting to store information offshore increases the vulnerability. To address this, organisations should observe best practices to ensure robust control over their offshore data, as outlined below.

Alternatively, keeping your data within local borders may help to minimise the risk of data breaches. The latter approach aligns more closely with community sentiments, as evidenced by the OAIC Australian Community Attitudes to Privacy Survey 2023 revealing that a substantial majority of Australian respondents (91%) expressed their reluctance to have their data sent overseas [5]. It's essential to remember that it only takes a single incident to shatter trust.

Data sovereignty best practices

Organisations looking to mitigate data sovereignty risks should consider the following best practices:

Understand your data flows

Firstly, organisations will need to have a clear understanding of their data flows, including where it is transferred, processed, and stored. A particular consideration is how data is handled and stored by third party vendors, especially if they provide cloud-based services or are otherwise located offshore. This can be achieved through a comprehensive data audit, which will enable organisations to identify potential data sovereignty risks and the applicable data protection laws and regulations.

Understand your obligations

The regulatory landscape of data sovereignty in Australia is murky. Laws range in scope from privacy to critical infrastructure to finance, to name a few. There is no uniform application of to whom these rules apply to; for example, the APPs apply to any APP entity handling personal information, while critical infrastructure legislation imposes positive obligations on responsible entities of data storage and processing facilities [6].

Further, as discussed in the "Data sharing vs. data localisation vs. data access" section, the requirements imposed by data sovereignty rules can vary from data sharing laws which permit the cross-border movement of data once certain requirements are meant, to data localisation laws which require the data to be hosted domestically.

Identifying the relevant data protection laws and regulations is not only essential to ensuring compliance, but also a crucial step in understanding the options your organisation has (what you can and can't do) when it comes to optimal data practices, especially when using cloud-based software and services.

Lastly, organisations must stay up to date with changes in data protection laws and regulations in the countries where they operate and adjust their data protection policies and practices accordingly. This includes being aware of changes in data protection laws and that affect how data is transferred, processed and stored, and who may have access.

The Implications of Data Sovereignty in Australia and Abroad

Understanding the data sovereignty laws can be a difficult task. We discuss some of the key Australian requirements below and in **Appendix A**.

Choose your cloud service provider wisely

A main issue challenging data sovereignty is the growing use of cloud services. These services enable their users to access a broad range of functionalities without needing to worry about the underlying infrastructure and maintenance cost. When compared to traditional IT infrastructure, cloud computing services are often more flexible, scalable, and cost-effective. Unsurprisingly, over recent years, cloud computing services have seen significant growth and widespread adoption.

Organisations should prioritise cloud service providers with data residency options. If available, the option of storing the information in Australia is a straight-forward and reliable choice that generally meets jurisdiction compliance requirements. This proactive approach to data localisation is a way of making your data and storage more secure and less likely to be subject to foreign control or interference. If the organisation must choose between other jurisdictions, it should first consider those with strong rule of law and robust privacy regulatory practices similar to Australia.

For some services, there is no option to choose where your data will be stored. If the location where the data is being stored seems appropriate for its use case, then it might be worth considering the services of other cloud providers, where organisations may have a choice to store their data in the region or location of their choice – e.g., as with Amazon Web Services, Google Cloud, IBM Cloud, or Microsoft Azure.

APRA regulated entities will be subject to certain outsourcing standards. APRA's own *Information Paper: Outsourcing involving cloud computing services* provides useful guidance on the risk considerations organisation should undertake such as security, governance, strategy, contingency planning and APRA access [7]. Similarly, the Office of the Victorian Information Commissioner has released their own risk assessment guidance *Cloud Computing in the Victorian Public sector* [8]. The document also highlights the importance of record keeping and ongoing assurance for agencies utilising cloud computing.

Ultimately, every organisation needs to ensure that the benefits of cloud computing are be balanced with its risks. It is necessary for organisations to calculate the financial impact of adopting cloud services from both upfront costs to long-term ongoing costs, while ensuring that data localisation is supported to maintain privacy compliance with the laws of the jurisdictions in which the organisation operates.

The Implications of Data Sovereignty in Australia and Abroad

Adopt robust data protection and security measures

Regardless of location, organisations must adopt robust data protection and security measures to ensure security is maintained and their data is protected appropriately. These include:

- Implementing a data protection policy, which aims to design, implement, guide, monitor, and manage security over an organisation's data
- Managing access controls, including multifactor authentication
- Implementing end-to-end encryption
- Monitoring, to ensure that sensitive and classified data is protected from unauthorised access, modification or use, and is not leaking, and
- Assuring the required outcomes via independent audits and/ or separate security assessment of third-party providers.

Further considerations for global organisations

There are additional considerations for organisations that engage globally, whether or not these organisations have multiple offices around the world or have their users located within one region. Global organisations must address, at a minimum, concerns with data localisation, cross-border transfers and government access as discussed below.

Foreign data localisation requirements

The level of data localisation protection varies from country to country, with some requiring certain types of data to be stored and processed within their borders (even if the organisation may not physically have a presence there). This can have vast implications for any international organisation that has its users located in multiple countries, since the requirements for handling of data (particularly, personal information of its users) can differ, and sometimes be conflicting, depending on the jurisdiction.

Cross-border data transfers

Ensuring the lawful and secure transfer of data across international borders remains a pressing concern, especially where there are multiple regulations (of variable levels of sophistication) to comply with. Organisations engaging in cross-border data transfers, including those with global offices or who are using cloud service providers, may experience increased costs and complexity in data management.

The Implications of Data Sovereignty in Australia and Abroad

Government surveillance and access

While governments have a legitimate interest in national security and law enforcement, it is essential to strike the right balance between these interests and the rights of individuals when faced with handing personal information over to authorities. Global organisations should be informed of the data privacy laws of the jurisdictions in which they operate, as well relevant surveillance or national security laws, particularly where there is potential for government authorities to access data with impunity.

Key questions for boards and executives

Data sovereignty is a prevalent and growing concern for organisations in an environment where there is increasing reliance on global trade and use of cloud services. The exposure of organisations to third (and foreign) parties means an introduction to new threats and the risk of data (including personal information) being exposed and exploited.

Additional considerations that need to be evaluated range from domestic data localisation laws and requirements to compliance with the data privacy laws of foreign governments. Overall, organisations must remain focused on compliance with domestic and international data privacy laws (as well as best practice) to retain user trust.

The considerations include:

- What data do we process and what is its sensitivity or criticality?
- What are the laws, regulations, or industry standards we must consider for this data?
- What are the company policies and user obligations we must meet as an organisation to handle this data safely?
- What measures have we taken to comply and manage risk associated with:
    - Data security, such as having a backup and disaster data recovery plan
    - Data access requests made by government authorities or, potentially, covert access
    - Geopolitical events and changing political climates?

Appendix A

Key Australian laws affecting data sovereignty

Privacy Act 1988 (the Privacy Act)

The Privacy Act allows organisations to store personal information with a cloud provider located in another State if certain requirements are met. Two parts of the Privacy Act apply:

- APP 8 – Cross-border disclosure of personal information [9], and
- APP 11 – Security of personal information, which requires organisations and agencies to take reasonable steps to protect personal information [10].

Apart from the requirements from APP 8, there are no general data sovereignty requirements in the Privacy Act – however, there are some requirements for specific sectors [11]:

- Under section 20E of the Privacy Act, credit providers who disclose credit eligibility information to offshore recipients without an Australian link must satisfy additional requirements, and
- Under section 77 of the *My Health Records Act 2012* (under the remit of the OAIC), My Health Record and associated information must not be held, taken, processed, or handled outside Australia. There is an exception where such data is non-personal or non-identifying information.

Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (aka TOLA)

TOLA is an overarching piece of legislation which gives government agencies the right of access to disrupt systems which can compromise national security.

Introduced in 2018, it provides Australian state, territory and federal law enforcement agencies with the ability to demand that "designated communications providers" create a capability for law enforcement agencies to intercept and monitor encrypted communications. TOLA remains under review and the Parliamentary Joint Committee on Intelligence and Security (PJCIS) has made recommendations to amend the legislation [12].

Designated communications providers are industry participants that might be subject to these requests. The definition is broad and includes [13]:

- Businesses who operate messaging platforms (e.g., Apple, Google, Reddit, Signal, X, WhatsApp, etc)
- Phone and internet service providers
- Technicians and retail repairers
- Developers of software used in connection with certain communication services
- Manufacturers of any component used in telecommunication equipment.

Appendix A

The Act applies to any company that develops, supplies, or updates software in connection with a communication service, and would apply to foreign companies that provide that relevant service.

The Director-General of Security, the Director-General of the Australian Secret Intelligence Service, the Director-General of the Australian Signals Directorate, or the chief officer of an interception agency may give the following types of requests to a designated communications provider [14]:

- A **technical assistance request (TAR)** may ask the provider to perform acts or do things on a **voluntary basis** that are directed towards ensuring that the provider is capable of helping ASIO, ASIS, ASD, or an interception agency in relation to safeguarding national security, the interests of Australia's national security and wellbeing, enforcing criminal law, etc.
- A **technical assistance notice (TAN)** may require the provider to perform acts or do things that are directed to towards helping ASIO or any other agency in relation to enforcing criminal law, so far as it relates to serious Australian offences, or assisting the enforcement of criminal laws in force in a foreign country, so far as those laws relate to serious foreign offences; or safeguarding national security. This is **a compulsory request**.
- A **technical capability notice (TCN)** may require the provider to perform acts or do things directed towards ensuring that the provider is capable of helping ASIO or an interception agency for the same reasons as above. This is a **compulsory request** requiring the provider to build a new capability for the agencies. Once built, the agencies can seek assistance with a TAN.

Surveillance Legislation Amendment (Identify and Disrupt) Act 2021 [15]

The law amends the previous *Surveillance Devices Act 2004* (Cth) and the *Crimes Act 1914* (Cth) and introduces new powers for the Australian Federal Police (AFP) and the Australian Criminal Intelligence Commission (ACIC) to access and 'disrupt' data held on computers to combat online crime with three new types of warrants:

- **Data disruption warrant**: Allows agencies to access data held on a computer. The law enforcement agency can apply for the warrant if it suspects on reasonable grounds that offences of a particular kind have been, are being, are about to be, or are likely to be, committed; and they involve data held in a computer.

Appendix A

- **Account takeover warrant**: Authorises the AFP or the Australian Crime Commission (ACC) to take control of a holder's online accounts if it suspects an offense and need to take control of the accounts in the course of the investigation to obtain evidence. This can be done covertly and without consent.
- **Network activity warrants**: Allows law enforcement agencies to access networks to enable the collection of intelligence that relates to criminal networks of individuals. The Digital Rights Watch is especially concerned that the definition used under this power is particularly broad and could "*enable widespread surveillance across social media and messaging platforms*" [16].

This relatively new law also permits law enforcement officers to apply for a warrant to require a specific person to provide any information or assistance that is considered necessary and reasonable. Organisations that supply data storage services or cloud services could be required to assist officers in the execution of these warrants. However, it should be noted that the organisation can object to disclosure if the information could reveal vulnerabilities in the organisation's system and technologies that could be used by others [17].

Security of Critical Infrastructure Act 2018 (SOCI Act)

The *Security of Critical Infrastructure Act 2018* (the SOCI Act) and amendments seek to manage the complex and evolving national security risks of sabotage, espionage, and coercion posed by foreign involvement in Australia's critical infrastructure. The Act applies to 22 asset classes across 11 sectors. **Data Storage or Processing** is one of the 11 sectors captured, with **Data Storage and Processing Facilities/Technology** being an especially relevant asset. The other sectors include: communications; defence; energy; financial services and markets; food and grocery; health care and medical; higher education and research; space technology; transport; and water and sewerage [18].

The SOCI Act provides that, among other things, 'positive security obligations' (PSOs) can be 'switched-on' and adjusted with rules for the 22 specified asset classes. There are three PSOs that can be 'switched-on':

1. **A requirement to provide ownership and operational information:** Details of critical assets to the Register of Critical Infrastructure Assets.

Appendix A

2. **A requirement to report cyber incidents:** Responsible entities must report cybersecurity incidents to the Australian Signal Directorate. Once an entity is aware of a cyber incident, it must be reported within 12 hours if having a significant impact on the availability of the asset, or 72 hours if having a relevant impact on the availability, integrity, reliability, or confidentiality of the asset.
3. **A requirement to maintain a Critical Infrastructure Risk Management Program:** The Department of Home Affairs indicates that "risk management program is designed to mitigate risks/hazards that can cause an impact on the functioning of critical infrastructure. For example, a terrorist attack on a major liquid fuel pipeline or data centre" [19]. The rules for the responsible entities for critical infrastructure assets are still being designed but are likely to contain the following requirements:
    a. **Cyber**: Ensure the risk management program includes mitigations that comply with specific standards and ensure that their risk management program includes details of a risk-based plan that outlines strategies and security controls as to how cyber and information security threats are being mitigated.
    b. **Personnel**: Ensure the risk management program includes details of how the entity implements appropriate background checking of new and ongoing employees, contractors and subcontractors, having regard to specific standards, and ensure the risk management program includes details of how the entity assesses and manages the ongoing suitability of its self-assessed critical employees, contractors and subcontractors.
    c. **Supply chain**: Ensure the risk management program includes details of how the entity complies with the business continuity components of specific standards and demonstrate how the risk management program, as far as is reasonably practical, minimises and mitigates relevant impacts to the asset arising from the supply chain [20].
    a. **Physical and natural**: Ensure the risk management program includes details of how the entity detects and controls unauthorised access and demonstrate in the risk management program how it conducts tests, as appropriate, to ensure active security measures are effective and appropriate.

Appendix B - Table of Australian laws, regulations, and guidance affecting data sovereignty

Relevant provision / guidance	Who	Data Type	Data Residency	Requirement(s)
***Privacy Act 1988* (Cth) APP 8 -** Cross-border disclosure of personal information [21]	APP entity	Personal information	**Data sharing –** Can be transferred overseas (if requirements met)	Take reasonable steps to ensure that the overseas recipient complies with APPs (satisfied with a contractual agreement). Exception if: reasonable belief of similar foreign legal scheme; there is express consent from individual; or as authorised by law or agreement; special situation (e.g., threat to life); or law enforcement.
***Privacy Act 1988* (Cth) APP 11 –** Security of personal information	APP entity	Personal information	**Data sharing –** Can be transferred overseas (if requirements met)	Take reasonable steps to ensure security of personal information. Offshore cloud services cited as a risk in cyber supply chain in the Australian Signals Directorate's **Australian Government Information Security Manual** [22].
***Privacy Act 1988* (Cth) s 20E**	Credit providers	Credit information	**Data sharing –** Can be transferred overseas (if requirements met)	Additional requirements apply before a credit provider can disclose credit eligibility information to offshore recipients who do not have an Australian link.
***My Health Records Act 2012* (Cth) s 77**	My Health system operators and related parties	My Health Records	**Data localisation –** Cannot be transferred overseas	My Health system operators and related parties must not hold, take, process or handle My Health Records outside Australia unless such information is deidentified or non-personal.
NSW PIPP Act s 19(2) – Transborder disclosure	NSW public sector agencies including government agencies, local councils, and universities.	Personal information	**Data sharing –** Can be transferred overseas (if requirements met)	Additional requirements apply before a NSW entity can disclose personal information to offshore recipients.

Relevant provision / guidance	Who	Data Type	Data Residency	Requirement(s)
Victoria PDP Act IPP 9 – Transborder data flow	Victorian public sector agencies including Ministers, local councils, statutory offices, government schools, universities, and TAFEs.	Personal information	**Data sharing –** Can be transferred overseas (if requirements met)	Additional requirements apply before a Victorian entity can disclose personal information to offshore recipients.
***Electronic Conveyancing National Law* (NSW) s 22**	Electronic Lodgment Network Operator (ELNO)	Any computer infrastructure forming the ELNO system	**Data localisation –** Cannot be transferred overseas	The ELNO must ensure that any computer infrastructure forming part of the ELNO System and in which Land Information is entered, stored or processed is located within the Commonwealth of Australia [23].
APRA CPS 231	APRA regulated entities	Any information involved in material business activities	**Data sharing –** Can be transferred overseas (if requirements met)	The entity must notify APRA before entering into a material outsourcing agreement. The entity must consult with APRA before entering into an off-shore outsourcing arrangement involving a material business activity or a use of use of cloud computing services involves heightened or extreme inherent risks. APRA may intervene and require the entity to make other arrangements. The entity must notify APRA as soon as the agreement has been entered into, and no later than 20 days, with a summary of the key risks and details of risk minimisation strategies in place. The outsourcing arrangement must also contain additional requirements to address the potential concerns with offshoring.

Relevant provision / guidance	Who	Data Type	Data Residency	Requirement(s)
APRA Information Paper: Outsourcing involving cloud computing services	APRA regulated entities utilising cloud computing	Any data used in cloud computing services	**Data sharing –** Can be transferred overseas (if requirements met)	Supports CPS 231 and provides resources for risk management considerations for cloud computing. Details the need to perform a materiality assessment, inherent risk assessment and offshoring assessment when determining whether to consult APRA on cloud computing use.
Department of Home Affairs Hosting Certification Framework	Service providers that deliver hosting services to sensitive government data	Sensitive and classified government data	**Data localisation –** Cannot be transferred overseas	A certified service provider must have its data centre located within Australia [24]. Additional requirements apply before a service provider can satisfy certification requirements.
***Security of Critical Infrastructure 2018 (SOCI) Act* (Cth) and Amendments**	Entities responsible for critical infrastructure	Any information that poses a material risk relating to a critical infrastructure asset	**Data sharing –** Can be transferred overseas (if requirements met)	The entity must detail a list of critical assets to the Register of Critical Infrastructure Assets. The entity must report cybersecurity incidents to the ASD within 12 hours of a significant impact, or within 72 hours of relevant impact. A Risk Management Program needs to be established to mitigate risks/hazards that can have a functioning impact to critical infrastructure. This specifically includes consideration of supply chains.
***Surveillance Devices Act 2004* (Cth)**	Entities that operate online	Any information related to the warrant	**Data access –** gives data access to government agencies	Grants the AFP and the ACIC three new powers to disrupt, collect, and take over data and accounts related to serious online crimes.
Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) *(aka TOLA)	Designated communications providers	Any information that poses a risk to national security	**Data access –** gives data access to government agencies	Gives new powers to Australian law enforcement and security agencies to access encrypted communications and data for the purposes of investigating and preventing serious crimes and threats to national security.

Bibliography

[1] M. Spiekermann, D. Tebernum, S. Wenzel, B. Otto (2018), pp. 326-337 cited M. Spiekermann (2019), Data Marketplaces: Trends and Monetisation of Data Goods, Intereconomics, ISSN 1613-964X, Springer, Heidelberg, Vol. 54, Iss. 4, pp 209.

[2] Macquarie Government, 'Data Sovereignty', <https://macquariegovernment.com/data-sovereignty/>.

[3] Australian Cyber Security Centre, 'Information Security Manual', <https://www.cyber.gov.au/acsc/view-all-content/ism>.

[4] Refer to the privacy principles on cross-border disclosure of personal information.

[5] https://www.oaic.gov.au/__data/assets/pdf_file/0024/74526/OAIC-Australian-Community-Attitudes-to-Privacy-Survey-2023-infographic.pdf

[6] *Security of Critical Infrastructure Act 2018* (Cth) Part 2C.

[7] https://www.apra.gov.au/sites/default/files/information_paper_-_outsourcing_involving_cloud_computing_services.pdf

[8] https://ovic.vic.gov.au/wp-content/uploads/2018/07/Cloud_Computing_in_the_Victorian_Public_sector.pdf

[9] Refer to Appendix B.

[10] Protective Security Policy Framework, <https://www.protectivesecurity.gov.au> and Australian Cyber Security Centre, 'Information Security Manual', <https://www.cyber.gov.au/acsc/view-all-content/ism>.

[11] Baker Mckenzie, Global Data Privacy & Security Handbook, 'Data Localization/Residency' (7 August 2023), <https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security/asia-pacific/australia/topics/data-localizationresidency> and
The Law Reviews, 'The Privacy, Data Protection and Cybersecurity Law Review: Australia' (8 October 2023), <https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/australia>.

[12] Parliament of Australia, Media Release, 'Review of TOLA (Assistance and Access) Regime' (22 December 2021), <https://www.aph.gov.au/About_Parliament/House_of_Representatives/About_the_House_News/Media_Releases/Review_of_TOLA_Assistance_and_Access_Regime>.

[13] Corrs Chambers Westgarth, Insights, 'Australia's new decryption legislation: What does it mean for you?' (10 December 2018), <https://www.corrs.com.au/insights/australias-new-decryption-legislation-what-does-it-mean-for-you>.

[14] Ibid.

[15] MinterEllison, Technical Update, 'How might the new Identify and Disrupt laws impact you?' (13 September 2021), <https://www.minterellison.com/articles/how-might-the-new-identify-and-disrupt-laws-impact-you>.

[16] Digital Rights Watch, 'Australia's new mass surveillance mandate' (2 September 2021), <https://digitalrightswatch.org.au/2021/09/02/australias-new-mass-surveillance-mandate/>.

[17] MinterEllison, Technical Update, 'How might the new Identify and Disrupt laws impact you?' (13 September 2021), <https://www.minterellison.com/articles/how-might-the-new-identify-and-disrupt-laws-impact-you>.

[18] Department of Home Affairs, 'Critical infrastructure resilience', <https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/critical-infrastructure-resilience>.

[19] Department of Home Affairs, Discussion Paper, 'Protecting Critical Infrastructure and Systems of National Significance', <https://www.homeaffairs.gov.au/reports-and-pubs/files/co-design-sector-specific-rules-discussion-paper.pdf> and Department of Home Affairs, 'Risk Management Program Rules' (26 November 2021), <https://www.homeaffairs.gov.au/reports-and-pubs/files/risk-management-program-rules.pdf>.

[20] Including but not limited to unauthorised access, interference or exploitation; privileged access; disruption and sanctions; threats to people, assets, equipment, products, services, distribution and intellectual property within supply chains; high risk vendors; and vendor dependency or reliance on entities inherently within supply chains.

[21] Office of the Australian Information Commissioner, Chapter 8: APP 8 Cross-border disclosure of personal information, 'When is an APP entity accountable for personal information that it discloses to an overseas recipient?' (22 July 2019), <https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information#when-is-an-app-entity-accountable-for-personal-information-that-it-discloses-to-an-overseas-recipient>.

[22] Australian Cyber Security Centre, 'Information Security Manual', <https://www.cyber.gov.au/acsc/view-all-content/ism>.

[23] NSW Operating Requirements for Electronic Conveyancing, <https://www.registrargeneral.nsw.gov.au/__data/assets/pdf_file/0011/1077284/NSW_Operating_Requirements_Version_6.1.pdf>.

[24] See Department of Home Affairs, Hosting Certification Framework, 'Certified Service Providers', <https://www.hostingcertification.gov.au/certified-service-providers>.

IIS Partners

INFORMATION INTEGRITY SOLUTIONS PTY LTD
PO Box 978, Strawberry Hills NSW 2012, Australia
P: +61 2 8303 2438
E: contact@iispartners.com
www.iispartners.com
ABN 78 107 611 898
ACN 107 611 898