Expanding Into Australia: Avoiding the Bite of Data Risk

FTI CONSULTING™

EXPERTS WITH IMPACT™

As you contemplate the compelling opportunities of expanding your business into Australia, alongside the promise of growth, you should also consider any data-related challenges. Much like the fearsome reputation of Australian wildlife, the perceived ‘danger’ of these challenges can be tamed through understanding and strategic risk mitigation.

Navigating Australia’s Data Landscape

In this booklet, we help you understand and navigate the landscape of data challenges, including the intricate terrain of the Australian Privacy Act 1998 and Spam Act 2003. We shed light on potential pitfalls and equip you with the knowledge and strategies to manage these risks. We aim to demonstrate that data risk in Australia is like the legendary venomous spiders: it’s best to avoid getting bitten but, if you’re prepared, even a ‘bite’ from a data threat actor should not be fatal to your business.

Situation Australia

In the past year, Australia has experienced a series of pivotal events that have reshaped the data risk landscape[1], including:

- high-profile public data breaches
- significant increases to penalties
- fresh government funding initiatives
- the establishment of new senior government positions
- the government’s recent stance on proposed privacy reforms.

The prevailing sentiment is that every corporate entity operating in Australia bears a solemn responsibility to safeguard the personal information of individuals. Any lapses in this regard are now met with swift and stern punitive measures, and public backlash. The Australian Government has displayed a heightened sense of urgency and unwavering determination to enforce compliance in areas of information governance, data privacy and security, leaving little tolerance for non-compliance.

Penalties for Privacy Act Breaches[2]

- AUD$50 million; or
- three times the value of any benefit obtained through the misuse of information; or
- 30% of a company’s adjusted turnover in the relevant period, i.e., the period of non-compliance, whichever is greater.
- Negative publicity
- Enforceable undertakings.

Penalties for Spam Act Breaches[3]

- Fines of up to AUD$1.1 million per day for non-compliant marketing messages
- AUD$11 million in spam and telemarketing breach penalties over the past 18 months
- Negative publicity
- Enforceable undertakings.

[1] Annual report highlights OAIC’s work to uphold privacy and information access rights. Office of the Australian Information Commissioner (19 October 2023)
[2] Tim de Sousa and Devina Potter. Australia Is Getting Serious About Penalties for Privacy Enforcement, FTI Consulting (31 October 2022).
[3] Investigations into spam and telemarketing Australian Communications and Media Authority (2 November 2023)

Corporate Opportunity

Australia boasts a vibrant technology market comprising both homegrown specialist solution providers and consultants. Major global players have also established local data centres for cloud solutions and international online collaboration and productivity tools. The global push for data-related legislative changes has catalysed the growth and maturation of the technical solutions sector. Consequently, a wealth of cost-effective and readily accessible solutions has emerged, breaking down barriers for businesses, large and small, venturing into the Australian market.

The synergy between technology and consulting services in Australia not only facilitates compliance but, perhaps more importantly, fosters the adoption of global best practices. This ultimately enhances the efficiency, effectiveness and safety of conducting business in the digital era.

This partnership yields additional advantages, including the capacity to remain agile in mergers and acquisitions. As buyers become increasingly attuned to data risks associated with business acquisitions, a lower level of data privacy and cyber maturity will directly impact their attractiveness to potential buyers or investors.

Key Data Risks

Over Retention

Excessive and unnecessary storage of data beyond its useful or legal retention period, which can lead increased storage costs and compliance issues, and exacerbate privacy incidents. This issue has been prominent in recent high-profile Australia data breaches. Many years of historic data needlessly retained, then stolen and exposed by threat actors.

Failure to Obtain Consent

An organisation or individual collects personal data from individuals without informed and valid consent. This action may infringe upon privacy rights, data protection regulations, and ethical standards, potentially leading to compliance consequences and loss of customer trust.

Sending Spam

When you send 'commercial electronic messages' (SMS or email), you must first have consent from the person who will receive them, identify yourself, and make it easy to unsubscribe from future messages. Failure to comply with these requirements can result in customer complaints, regulatory investigations, fines, and lengthy and onerous enforceable undertakings.

Key Data-Related Australian Regulators and Bodies

OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER (OAIC)

Independent national regulator for privacy and freedom of information. The OAIC has powers to instigate, litigate, and apply penalties under the Privacy Act. The OAIC is also the submission route for mandatory breach reporting obligations.

oaic.gov.au

AUSTRALIAN COMMUNICATIONS AND MEDIA AUTHORITY (ACMA)

Regulates communications and media to contribute to maximise the economic and social benefits of communications infrastructure, services and content for Australia. ACMA has powers to apply penalties and enforceable undertakings for breaches of the spam act.

acma.gov.au

AUSTRALIAN SECURITIES AND INVESTMENTS COMMISSION (ASIC)

Australia's integrated corporate, markets, financial services and consumer credit regulator. ASIC will take legal action if an entity breaches its licence obligations for failing to adequately manage its cybersecurity risks.

asic.gov.au

AUSTRALIAN PRUDENTIAL REGULATION AUTHORITY (APRA)

Responsible for ensuring that the Australian financial system is stable, competitive and efficient. APRA will enforce security standard for financial institution.

apra.gov.au

AUSTRALIAN SECURITY INTELLIGENCE ORGANISATION (ASIO)

Protects Australia and Australians from threats to their national security. In the event of a data breach, all government IDs breached may need to be reported to ASIO.

asio.gov.au

AUSTRALIAN CYBER SECURITY CENTRE (ACSC)

The Australian Signals Directorate's ACSC leads the Federal Government's efforts to improve cybersecurity. In key industries identified by the Security of Critical Infrastructure Act, there are mandatory reporting obligations to the ACSC in the event of a Cyber incident which impacts critical infrastructure assets.

cyber.gov.au

Next Steps

Against an increasingly volatile and evolving regulatory landscape, companies are seeking to proactively mature their data risk posture by better understanding what data they hold, where it's located, and the relevant legal retention periods. We're seeing various service trends from our clients, including:

Data Mapping

Gaining valuable insight into your data collections, holdings, transfers, disposals, and importantly, your high-risk data repositories. Effective data mapping can support better operational and compliance outcomes in both your existing practices and your proposed Australian expansion.

Privacy Impact Assessments

Assessing, understanding, mapping, and mitigating privacy risks within key strategic initiatives. These assessments enable businesses to demonstrate care and consideration in the use and handling of valuable consumer data, and to enable privacy-by-design.

Privacy Policy Framework Uplift

Ensuring your policy framework is accurate, up-to-date, and fully compliant with Australia and the other regions where you currently operate. A developed framework supports implementation of best privacy practice throughout the organisation. It also enables the demonstration of defensible compliance to regulators

Spam Act Compliance

Making sure you and your marketing team understand your obligations and implement appropriate systems and processes to avoid any expensive and reputationally costly infringements as you enter the new market.

Data Remediation

Proactively remediating and managing any existing over-retained data, including live unstructured and structured data, backups, migration collateral, legacy systems, and even magnetic data tapes.

Data Breach Readiness

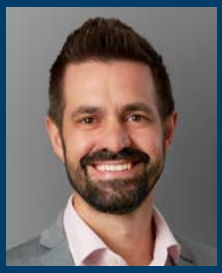
Proactively planning for data loss events by running breach event simulations and uplifting crisis response plans. Onboard providers to support post-breach events with investigations, crisis communications, and rapid assessments of exposed data for notifications and reporting.

Supporting Your Broader Needs

As well as helping you navigate the data risks and benefit from the opportunities of entering the Australian market, FTI Consulting provides additional services to support your business.

- ESG & Sustainability
- Data Privacy
- Corporate Reputation
- Cybersecurity
- Economics & Valuations
- Business Intelligence & Due Diligence
- Transactions, Turnaround, Acquisitions & Divestitures

To learn how you can successfully navigate the Australian data risk landscape, contact:



CHRISTOPHER HATFIELD
Data Risk & Information Governance
+61 437 373 130
christopher.hatfield@fticonsulting.com

TIM DE SOUSA
Privacy & Technology Ethics
+61 413 248 107
tim.desousa@fticonsulting.com

EXPERTS WITH IMPACT™

FTI CONSULTING™