Article Information

Author: Craig Subocz
Service: Cyber Security, Dispute Resolution & Litigation, Intellectual Property, Intellectual Property & Technology, Privacy & Data Protection
Sector: IT & Telecommunications

Managing Data Risk in a Technology-Driven Environment: Why Governance Matters More than Ever

How organisations create, use and store data has changed dramatically over time. From the rise of personal computing in the 1980s, through the internet and "big data" eras, to today's cloud-based, AI-driven environment, data is now one of the most valuable and risky assets a business holds.

During our March 2026 Digital Law Series webinar, we explored how boards and executive teams can better manage data risk in an increasingly complex legal landscape. The webinar highlighted a common challenge – organisations recognise that data is critical, but many are unsure whether their governance frameworks are keeping pace with the evolution of technology.

This webinar and previous Digital Law Series webinars are available to be watched on demand through the Piper Alderman website.

This insight highlights some of the key takeaways from the webinar.

Data Governance is no longer optional

The sheer amount of data being generated globally is staggering. By one calculation, over 180 zettabytes of data would have been generated worldwide. Multimedia content – video, images and social media – now accounts for the vast majority of internet traffic. For the sake of context, one zettabyte is equivalent to the content of approximately 250 billion DVDs.

In this context, how data is generated is often what separates resilient, trusted organisations from those exposed to regulatory, cyber and reputational risk.

Data governance is not just an IT issue. It is a matter of stewardship. Every business owns certain data assets. These might be structured (such as data held inside CRM and finance systems) as well as unstructured (such as data in emails, documents, images and videos). They often embed confidential, personal and/or sensitive information. Under Australian law, boards already have obligations to oversee how those assets are managed, particularly where personal information is involved.

Therefore, if your organisation holds valuable data (and it probably does), governance sits squarely within the remit of the board.

The Board's Role in Data Stewardship

A recurring theme in our recent webinar was accountability. Ultimately, responsibility for data governance sits with the board, since it falls within the scope of the existing directors' duties under the *Corporations Act* and the common law.

One approach to effective data governance is to adopt the following five key principles:

- Treat data as the company's strategic asset;
- Define clear governance and accountability for data governance;
- Manage risk throughout the data lifecycle;
- Empower a data-driven organisational culture;

- Ensure effective data incident response and recovery

These principles set out a practical approach for boards to ask the right questions internally:

- What data does the company hold, why does the company hold that data, and where is that data stored?
- Are decision-makers confident in the quality and accuracy of that data?
- Does the company understand how third party service providers handle the company's data?
- Critically, is the company prepared when something goes wrong?

By asking and seeking answers to these questions, the board can assess whether the data governance policy adopted by the company is fit for purpose, or whether it requires adjustment to take into account the particular circumstances faced by the company.

Privacy Governance: More than just a Policy on a Website

A common misconception is that compliance with the *Privacy Act 1988* (Cth) starts and ends with a privacy policy posted to a website. Australian law requires companies not only to publish an up-to-date privacy policy, but also to take reasonable steps to implement "practices, procedures and systems" to ensure compliance with the company's statutory obligations. This internal dimension can be where companies fall short.

Complementing the data governance approach is a framework for effective management of privacy obligations. This requires four interconnected elements to be brought together:

- Evaluation and oversight (audit, risk and board reporting)
- Governance and leadership (strategy, culture and accountability)
- Complaints and incident management (including breach response and dealing with aggrieved individuals)
- Operational privacy programs (policies, training and contracts)

When these elements all operate cohesively, with the benefit of clear board endorsement, privacy compliance becomes embedded in the culture of the company, rather than being an after-the-fact response.

The impact of AI on data governance

Generative AI technology does not exist in isolation. The technology consumes data, generates new data and often blur traditional boundaries around use and disclosure.

A key risk for any organisation considering the adoption of AI tools is that they do so without a clear understanding of how those tools interact with existing data governance settings. Publicly available AI tools, in particular, raise questions regarding confidentiality of critical or sensitive business information, the risk of data leakage and the loss of legal professional privilege.

From a privacy perspective, the use of generative AI tools can directly engage multiple Australian Privacy Principles, including those dealing with the collection of personal information, the use of personal information, accuracy and transparency.

The essential takeaway for boards and executives is clear: AI should be treated as a data governance issue, not merely a technology upgrade. If the underlying data practices are week, AI will amplify the problem.

"AI by default" and third party risk

Another emerging area of risk we discussed is the quiet rollout of AI functionality within common business tools. Features could be enabled by default, with limited visibility as to how data is processed or retained. Companies should be proactive in identifying where AI is embedded in existing platforms or systems and disabling or restricting it until privacy, security and risk settings are properly assessed.

It also underscores the importance of third party governance. Contractual confidentiality promises on their own may be insufficient. Boards should expect and require visibility over vendor data handling practices, realistic contractual protections and clear incident response obligations.

Can data ever really be deleted?

The question of deletion is a tricky one to answer. Whether data can ever really be deleted depends on several factors. In modern digital environments, data is often copied across systems, backups and logs. It may even be incorporated into board papers. Accordingly, deletion of data could be logical rather than physical, and residual copies might persist.

From a governance perspective, the focus should be on reasonable, defensible practices, rather than absolute guarantees. Transparency in privacy statements and accuracy in internal processes are critical, as well as carefully considering deletion obligations in non-disclosure agreements.

Looking forward: data governance as an enabler

Good data governance is not merely a defensive exercise. When done well, it enables better decision-making, builds trust with stakeholders and supports responsible innovation.

As technology continues to evolve, boards that actively engage with data governance (as opposed to simply delegating it entirely) put their organisations in a comparatively far stronger position to manage risk and capture opportunity.

With a greater emphasis on the transparency of the use of personal information in automated-decision making that has a "significant impact" on the rights or interests of individuals, organisations should critically review their data governance approach and revise them as appropriate to ensure that they maintain compliance with relevant laws.