ORGANISATION

Data and privacy governance

Technology has supercharged the collection and processing of data. Directors and boards are responsible for directing their organisations to leverage data-driven opportunities while ensuring appropriate governance of their data.

For the purposes of this tool, data governance refers to the processes, systems and frameworks for using and managing data to:

- improve an organisation's internal functioning; and
- help an organisation pursue valued goals and objectives.

Privacy governance encompasses the above as applied to 'personal information' under the *Privacy Act 1988* (Cth) (Privacy Act), which is a subset of data relating to someone who is identified or reasonably identifiable.

The following sections outline the evolving regulatory landscape on data and privacy governance and its implications for boards, as well as provide questions to assist directors to understand and discharge their responsibilities in relation to this critical and growing area of governance.

Evolving regulatory landscape and its implications for boards

In Australia, the Privacy Act is the one existing law that broadly prescribes how data (specifically, personal information) is used and managed. It does this through the 13 Australian Privacy Principles[1] (APPs).

APP 1.2 specifically calls on organisations to take reasonable steps to implement practices, procedures and systems that will ensure compliance with the APPs.

The Office of the Australian Information Commissioner (OAIC) has published a Privacy Management Framework[2] (PMF), which sets out the steps that it expects organisations to take in relation to APP 1.2. Importantly for directors, the first step is for the organisation's leadership and governance arrangements to create a culture of privacy that values personal information.

1 Office of the Australian Information Commissioner, 2019, *Australian Privacy Principles*, Australian Government, [website], https://www.oaic.gov.au/privacy/australian-privacy-principles/, (accessed 5 December 2019).

2 Office of the Australian Information Commissioner, 2015, *Privacy management framework: Enabling compliance and encouraging good practice*, Australian Government, [website], https://www.oaic.gov.au/privacy/guidance-and-advice/privacy-management-framework-enabling-compliance-and-encouraging-good-practice/, (accessed 5 December 2019).

Directors' responsibility in promoting good privacy culture and practice is more important than ever, in light of recent government pledges to enhance the penalty regime under the Privacy Act (including fines of up to 10 per cent of a company's annual domestic turnover) and to provide additional funding to the OAIC to conduct its regulatory work.

Going beyond personal information, there have been several inquiries, reviews and reports in the mid-to-late 2010s examining the use and availability of data more generally. The most consequential one has been the Productivity Commission's Data Availability and Use Inquiry, which investigated ways to improve the availability and use of public and private sector data.

In response to the final report published in May 2017[3], the Australian Government has committed to two major legislative reforms with implications for data governance.

Firstly, the Government is drafting a new Data Sharing and Release Act (DS&R Act) that will allow government agencies to share public sector data with trusted users in a controlled way, for non-commercial purposes.

Directors of organisations in the not-for-profit and research sectors should ensure that their internal data governance measures align with the requirements for becoming a trusted user. More generally, directors should consider how their organisation is positioned to take advantage of the greater availability of open public sector data.

Secondly, the Government is in the process of implementing a new data sharing regime that affects private sector data – the Consumer Data Right (CDR)[4]. The CDR allows consumers to access certain data held about them by businesses and to transfer this to trusted third parties in order to obtain a benefit, such as receiving a better deal or a new service.

The CDR will be introduced on a sector-by-sector basis, starting with banking and followed by energy and telecommunications, with the eventual goal of applying economy-wide. Directors should note that in the first phase, the CDR applies not just to banks but also organisations who have been accredited to receive CDR data in order to provide a product or service, as well as to outsourced service providers that handle such data.

The Australian Competition and Consumer Commission (ACCC) is making rules on the rights and obligations of CDR participants that supplement the privacy safeguards introduced by the CDR Bill. Together they have strong implications for data governance:

- Consumers must expressly consent for the transfer and use of their data;
- The privacy safeguards mirror the structure of the APPs but are more stringent in some areas; and
- Schedule 1 to the CDR Rules prescribes specific steps to protect CDR data, including:
  - having a formal governance framework for managing information security risks; and
  - documenting specific responsibilities of senior management (that is, directors) for the protection and management of CDR data.

These developments are an indicator of the regulatory landscape to come. The following sections provide guidance on how to think about and approach data governance from the board's perspective.

3 Productivity Commission, 2017, *Data Availability and Use: Productivity Commission Inquiry Report*, No 82, Australian Government, 31 March, https://www.pc.gov.au/inquiries/completed/data-access/report/data-access.pdf, (accessed 5 December 2019).

4 Office of the Australian Information Commissioner, 2019, *About the Consumer Data Right*, [website], 29 November, https://www.oaic.gov.au/consumer-data-right/about-the-consumer-data-right/, (accessed 5 December 2019).

Framework for data and privacy performance

One way to conceptualise data and privacy governance is using the data and privacy performance (DPP) framework, which was introduced in *The New Governance of Data and Privacy*[5], published by the AICD (refer to Figure 1). While the framework focuses on personal information (which, as noted above, comes with compliance obligations), it can readily apply to other valuable organisational data.

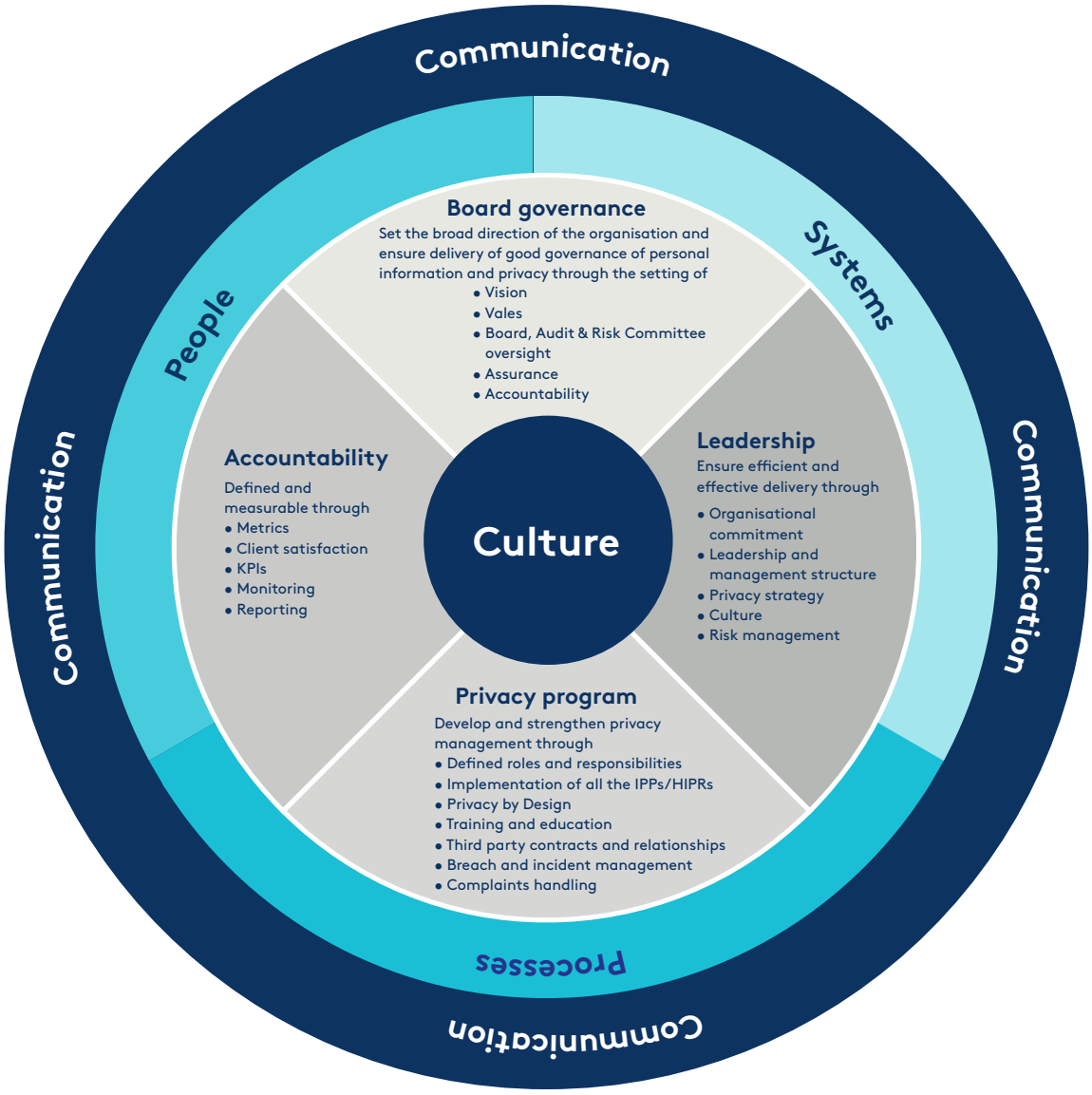

Figure 1: Framework for data and privacy performance

5 M Crompton and M Trovato, 2019, *The New Governance of Data and Privacy*, AICD, p 40, https://aicd.companydirectors.com.au/resources/bookstore/the-new-governance-of-data-and-privacy, (accessed 5 December 2019).

Having a clear DPP framework allows the board to exercise oversight and control over how the organisation uses and manages data as a key asset. Without such a framework, organisations are more prone to mishandle their data while simultaneously failing to leverage it for new opportunities.

There are three elements of the DPP framework with which directors should familiarise themselves:

- strong organisational culture;
- effective structures – board governance, executive leadership, privacy program and accountability; and
- supporting infrastructure – people, processes, systems and communication.

At the heart of the framework is a strong organisational culture for respecting privacy and using data in a creative and trustworthy way. Such a culture requires an effective structure in order to embed privacy considerations into everyday practice and decision making.

An effective structure starts with board governance. The board establishes and communicates the values of the organisation, its strategic vision and risk appetite. This sets the bounds for how the organisation uses and manages its data, as well as the requisite maturity level of its people, processes and systems.

The executive leadership team is responsible for carrying out the organisation's functions and activities, including data handling, in line with the board's governance.

The privacy program represents the steps that an organisation must take to ensure compliance and facilitate good practice in accordance with the board's position. These steps can incorporate regulator guidance (such as the PMF above), industry practice and international standards.

Completing the effective structure is accountability, which takes the cycle back to the board level. The board is responsible for ongoing monitoring of the organisation's data handling practices, including its privacy program and the actions of key personnel.

Surrounding and supporting the organisation's culture and structure are its people, processes and systems. These are the fundamental enablers that give expression to the organisation's data and privacy aspirations.

Finally, effective communication – from the board, throughout the organisation, and back to the board – is required for the DPP framework to function in practice.

As expanded on below, the DPP framework provides a good springboard for the board to consider its role in data governance.

How does a board fulfil its role in data and privacy governance?

The time and focus a board dedicates to data and privacy governance will depend on such things as the organisation's size, the quantity and quality of its data holdings, industry and strategic direction. The basic steps, however, are the same.

1. **Foster a culture that values data and privacy**
   Have the values and risk appetite underpinning data handling been established and communicated throughout the organisation? Is the organisation appropriately equipped and resourced to embed the right culture into its people, systems and processes? What channels does the board use to ensure it knows how data handling is occurring 'on the ground'?
2. **Future-proof the board**
   How do new data-driven business models and value chains enhance, or threaten, what the organisation is doing? What new technologies can be deployed to enable the organisation to do more with, and to protect, its data assets? What new laws must the organisation adhere to, and what frameworks, standards and guidelines should the organisation take heed of? Amid all the change, what are the attitudes and mindsets of individuals, stakeholders, regulators and lawmakers?
3. **Appoint key personnel and hold them accountable**
   Does the organisation have key data and privacy roles and responsibilities at the operational and leadership levels? How should resources and staff be allocated in terms of compliance (protecting data) and performance (leveraging data) functions? What are the reporting requirements and key performance indicators?
4. **Enhance privacy and security resilience**
   How ready is the board and executive to deal with a data-related crisis? How can the board improve its resilience capabilities, such as change readiness and incident management? Are privacy and security risks accounted for throughout the organisation and in project development? How are third-party relationships managed, secured and assured?
5. **Focus on your stakeholders**
   Does the board consider a wide range of stakeholder perspectives when making decisions about data? Is stakeholder-care a key value? Does this align with actual practice and is it communicated externally? What should the organisation do, or stop doing, to enhance stakeholder trust?

How can a director assess the effectiveness of data and privacy governance?

A good starting point is for directors and boards to self-assess their data and privacy governance practices by asking questions such as:

- Is the board regularly briefed on the risks to the organisation associated with data handling, in particular of personal information?
- Is data and privacy a regular item on the agenda of the board and is it addressed in a structured manner?
- Does the board have a clear view on major investments in data projects from a risk and return perspective?
- Does the board obtain regular progress reports on major data projects?
- Is the board getting independent assurance on the achievement of data objectives and the containment of data risks?

Based on the DPP framework, the board can consider the following ways of assessing performance:

- Culture – Conduct a culture 'stocktake' via interviews, surveys and meetings with a representative sample of staff across divisions and levels of the organisation.
- Board governance – Self-assess according to the questions in this guide; ensure data and privacy are regular board agenda items.
- Executive leadership – Obtain regular updates from leadership on the implementation of data-related programs and initiatives for which they are accountable.
- Privacy program – Obtain regular updates on the implementation and progress of relevant aspects of the privacy program (for example, refresher training conducted; privacy complaints received; third-party contracts reviewed, etc.).
- Accountability – Ensure that leadership is reporting at sufficient intervals, and to a sufficient level of detail, on data-related matters.
- People – Conduct, and participate in, assessments and scenarios to determine current data handling competency (for example, in the ordinary course of work, developing a specific project, when something goes wrong, etc.).
- Processes – Seek assurance that effective internal processes exist to meet compliance requirements and organisational goals at all stages of the data lifecycle (such as collection, use, disclosure, retention and disposal).
- Systems – Seek assurance that the organisation's systems are subject to appropriate security controls and that all data holdings are accounted for.
- Communication – While assessing the above, consider the extent to which each component has been helped by good communication or hindered by poor communication.

How can directors improve their data and privacy governance?

The first step to improving data and privacy governance is a review of existing competencies and capabilities within the organisation and at the board level. The DPP framework is a helpful reference point for this step.

Specific steps for directors include:

- Set a good personal example in data handling practices and participate in internal initiatives such as privacy training and incident response scenarios.
- Improve director competency through appointment of new directors or education of existing ones on data handling.
- Establish an additional committee or advisory group with a particular focus in this area.
- Review the range of delegations established by the board and formalising responsibility and accountability for data and privacy governance.
- Seek guidance at board meetings from knowledgeable internal staff or external experts.
- Hold periodic (for example, annual) planning sessions to discuss internal and external environments and the implications for data and privacy governance.
- Apply a future-minded data lens to deliberations and decisions at the board level - How does our values and risk appetite inform the issue at hand? How does the changing environment and our data assets affect strategy formulation? What practices or processes need to be introduced or changed to facilitate this?

Ten key questions for directors and boards on data and privacy governance

1. Given the technological, business and regulatory environment, in what ways is the data the organisation holds an asset? In what ways can the data be a liability for the organisation?

2. Given the organisation's data holdings and business aspirations, what knowledge and expertise does the board require to help it make decisions about deriving value from, and protecting, the data?
3. What is the organisation's current privacy stance (that is, the attitude and approach to handling personal information)? What is the organisation's desired privacy stance and how will directors, with the help of the executive team, implement and communicate the desired stance and the strategy for change?
4. Do directors understand the implications of the Privacy Act (including the OAIC's PMF under APP 1.2 and the Notifiable Data Breaches scheme) and, where relevant, the EU's General Data Protection Regulation? Are there additional steps the organisation's needs to take?
5. Are there clear roles, groups and lines of responsibility for data management that are appropriate to the size and value of the organisation's data holdings? Does the board hold them to account?
6. To what extent do the key control areas (for example, risk, compliance, internal audit) have a data and privacy ambit, and do directors ensure that those areas are properly managed, resourced, represented and emphasised at the board level?
7. How well are privacy processes and controls being executed? Does the organisation have a systematic way of finding out and is this regularly communicated to the board?
8. Are there metrics about privacy performance, and does the board ensure that they play a role in determining incentives within the entity?
9. Do directors discuss stakeholder needs, expectations and interests around data at board meetings? Do directors take them into account when making decisions?
10. Do directors know the ways that the organisation is (or isn't) earning stakeholder trust and building social licence? How can the organisation improve in this regard?

AISA Australian Information Security Association

About AISA

The Australian Information Security Association (AISA) champions the development of a robust information security sector by building the capacity of professionals in Australia and advancing the cyber security and safety of the Australian public as well as businesses and governments in Australia.

For more information **t:** +61 2 8076 6012 **w:** aisa.org.au

About AICD

The Australian Institute of Company Directors (AICD) is committed to strengthening society through world-class governance. We aim to be the independent and trusted voice of governance, building the capability of a community of leaders for the benefit of society. Our membership includes directors and senior leaders from business, government and the not-for-profit (NFP) sectors.

For more information **t:** 1300 739 119 **w:** aicd.com.au

07236-3-28-122019