Privacy Act Compliance

An entity should have a robust compliance program surrounding its privacy policies and procedures. An effective compliance program will facilitate the execution of legal obligations and will aid a due diligence defence in the event of a breach occurring.

> *Regulatory compliance is the management discipline of designing and implementing effective steps to ensure that an entity actually complies with the laws, regulations and codes of practice relating to its operations.*

- Personal Information (PI) – information about an individual which identifies that individual.
- Sensitive Information (SI) – PI about race, ethnicity, political, religious, philosophical views, sexual orientations, practices, criminal records, health, genetic, biometric information.

If compliance is being managed competently by management and monitored appropriately by the Board (or by a subcommittee) then the risk of non-compliance should be low as adherence to legislation is considered an administrative task.

Privacy of PI &/or SI is a significant issue for directors and boards, and even more so now due to new technology that enables many powerful and varied uses of this data, as well as its flow and distribution.

On 12 March 2014, sweeping new amendments to the Privacy Act came into effect. Not only must ***Boards*** comply with the new Australian Privacy Principles (APPs), they ***need to demonstrate this compliance***.

Be aware, forthcoming legislation may impact the entity. The Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 sets out mandatory data breach notification requirements for business and government entity's to inform consumers or taxpayers if their private information was lost or stolen.

Most entities collect (PI) &/or (SI) relating to employees, shareholders, members, volunteers, customers, etcetera. Therefore, read through the following questions and then ***request management to respond*** to them at an upcoming Board/subcommittee meeting (allow sufficient time for management to gather the required information).

1. Does the entity have an up-to-date privacy policy – when was it last reviewed by management and approved by the Board?

2. Does the privacy policy guide management in designing and implementing effective steps to ensure it actually complies with the privacy legislation relating to its operations and of member clubs/branches?

3. Does the entity collect personal information?
   a. Has a data inventory been completed? A data register detailing the data fields (mandatory & optional), necessity, usages, accessibility, etcetera.
   b. Is any of the information sensitive enough to require a higher standard of protection?

4. When did the Privacy Officer last conduct an audit which documented (or confirmed) where and how PI &/or SI is held by the entity and the way it is handled? Matters that should be documented are:
   - How the information is collected.
   - In which format the information is held.
   - When individuals are provided with the entity's privacy statement. Is a register maintained.
   - How the information is used within the entity.
   - Who has access to PI &/or SI.
   - What are the IT security protocols employed at each level of user access.
   - How can the information be accessed (e.g. computer, smartphone, internet, hard copy).
   - How is the database maintained.
   - How is the database validated.
   - What is the program for database validation.
   - What features protect the information from being given to others (e.g. methods preventing the exporting of information to another format/program).
   - What is the physical security that protects the hardware containing the PI &/or SI.
   - Who by and when can information be deleted. Is there a deletion policy.
   - Whether any PI &/or SI is sent overseas. If so, how is it controlled.

5. Has the privacy compliance audit been reviewed/audited by a third party for validity and completeness?

Privacy Act Compliance

6. In the event of a data breach, does the entity have a privacy data breach management plan?
   a. If so, who maintains the plan?
   b. When was the plan last reviewed?
   c. When was the plan last presented to the Board or subcommittee?
   d. Does the plan describe when individuals will be notified of breaches affecting them?

7. What are the remedial actions prescribed by the Board when there is a privacy breach?

8. Have there been any known, alleged or suspected privacy breaches recorded by the entity over the past several years?
   - What were the responses to the breaches and what lessons were learned to prevent future breaches (should be documented)?

9. Do privacy system administrators have appropriate security clearances or undergo security vetting?

10. What training is provided to those who can access PI &/or SI and what training records are maintained and by whom?
    - Is privacy training, tailored to roles and responsibilities, mandatory for all employees and contractors who can access PI &or SI?

11. Does the entity outsource any functions that allow a contractor to access PI &/or SI that the Board remains liable for?
    a. Are privacy requirements built into contractual agreements with business partners and service suppliers and agents?
    b. Do staff dealing with contractors (outsourced functions or other third parties) have access to specific policies and procedures guiding them on access contractors are allowed?

12. What systems are in place to monitor adherence to the privacy compliance program by all who can access PI &/or SI?
    - Is there an internal privacy audit program to ensure staff comply with the entity's privacy policies?

13. Are there triggers in the system to initiate a review prior to the implementation of a change management program, that is, before new services or processes are introduced?

14. How is the entity keeping abreast of new legislation?
    a. When was the legislation last updated by the regulator?
    b. What is management's program to keep themselves informed of legislation changes?
    c. Has the privacy policy been reviewed against the current legislation within the last 12 months?

15. Is performance of both the entity and all staff (particularly senior staff) measured against the entity's privacy compliance program?

16. Does the entity have adequately resourced privacy personnel or a team to deal with operational privacy issues such as complaints, access requests, corrections and compliance in general?

Board Specific Review

- Does the entity have an information management strategy reflecting the board's commitment to privacy and the importance of personal information to the entity? Is there:
  a. A senior role with management responsibility and accountability for privacy information handling?
  b. A comprehensive internal privacy policy that reflects the operations of the entity?
  c. An appropriate weighting for privacy and the management of personal information in the entity's overall risk management framework?

- Considering the size of the entity, is there sufficient oversight of privacy by the Board or a subcommittee about information management and privacy?

Sources:

- AICD Publication: Privacy Governance: A Guide to Privacy Risk & Governance for Directors and Boards
- Risk & Compliance Course Notes – Governance Institute of Australia
- Further detailed information can be obtained from the Office of the Australian Information Commissioner https://www.oaic.gov.au/agencies-and-entitys/guides/guide-to-securing-personal-information#part-b-steps-and-strategies-which-may-be-reasonable-to-take