Allens Privacy Checklist

Remember to consider the specific circumstances of your entity and check for any additional requirements.

☐ Review and update privacy policies

- ☐ Include in your entity's privacy policies the following required information:
  - reference to any significant information handling practices or specific requirements on your entity;
  - how an individual may access personal information about the individual that your entity holds, and seek correction of that information;
  - how an individual may complain about a breach of the Australian Privacy Principles (***APPs***) or a relevant registered code, and your entity will deal with such a complaint; and
  - whether your entity is likely to disclose personal information to overseas recipients, and if practicable, the countries in which those recipients are likely to be located.
  - Put procedures in place for privacy policies to be regularly reviewed and published on your entity's website.

☐ Review and update collection statements

- ☐ Add the following matters to collection statements which are provided to individuals on collection of personal information:
  - if the information is collected indirectly or the individual may not be aware of the collection, the fact that information is being collected and the circumstances of the collection;
  - any court/tribunal order that requires collection;
  - that your entity's privacy policy contains information about:
    - access to and correction of personal information held by your entity; and
    - how to complain about breaches of the APPs or any relevant registered code, and how complaints will be dealt with; and
  - whether your entity is likely to disclose the personal information to overseas recipients and, if practicable, the countries in which such recipients are likely to be located.

☐ Identify cross-border disclosures and review applicable arrangements

- ☐ Analyse whether the change from National Privacy Principle 9, which regulated 'transfer' of personal information outside Australia, to APP 8 which uses the broader term 'disclosure', means that there are additional disclosures with which your entity will now need to comply.
- ☐ In relation to all overseas disclosures your entity currently makes (including if the recipient is a related body corporate), consider whether your entity is or will be taking all steps as are reasonable in the circumstances to ensure the overseas recipient does not breach the APPs.
- ☐ Consider, in relation to any overseas disclosures, whether any of the exceptions to the principle that your entity remains accountable for breaches by the overseas recipient may be able to be satisfied. If the exceptions will not be satisfied, consider the warranties and indemnities available to your entity under its contracts with overseas recipients, including in relation to acts by subcontractors of overseas recipients.

☐ Review direct marketing procedures

- ☐ Where your organisation currently markets directly to certain individuals, consider in respect of each individual whether:
  - the individual has expressly consented to the direct marketing or would otherwise reasonably expect their personal (non-sensitive) information to be used for direct marketing; or
  - your organisation is required to perform direct marketing to those individuals under a government contract.

  If not, consent may be required in order to continue marketing to those individuals.
- ☐ When engaging in direct marketing, ensure any necessary consents are sought and any required opt-outs and notices are given.

☐ Review and update procedures

- ☐ Introduce procedures for dealing with unsolicited information, to ensure that an appropriate privacy, legal or compliance officer is notified when unsolicited information is received and an assessment is made as to whether the information could have been collected if it had been solicited.
- ☐ Consider adopting an internal policy and procedures to promote privacy compliance and monitoring your entity's practices to ensure they align with those policy and procedures.
- ☐ Consider introducing compulsory privacy compliance training, in particular for those employees who regularly deal with personal information.
- ☐ Consider introducing a requirement that privacy impact assessments be conducted when a new business or corporate initiative is under consideration.

☐ Credit Reporting Code

There are further changes which apply to organisations that provide credit or to credit reporting bodies.

The requirements are binding on most credit providers and significantly impact on systems used to handle information about credit.