THE LAW SOCIETY
OF NEW SOUTH WALES

Our ref: PDL:JBml170325

17 March 2025

Dr James Popple
Chief Executive Officer
Law Council of Australia
PO Box 5350
Braddon ACT 2612

By email: natalie.cooper@lawcouncil.au

Dear Dr Popple,

COMMONWEALTH DATA RETENTION REVIEW

Thank you for the opportunity to contribute to the Law Council of Australia's submission in response to the Commonwealth Data Retention Review Discussion Paper (**Discussion Paper**) issued by the Department of Home Affairs and Department of Attorney-General (**Departments**). The Law Society's Privacy and Data Law Committee and In-house Corporate Lawyers Committee contributed to this submission.

We note that the scope of the Review is limited to data retention provisions in primary and secondary Commonwealth legislation that directly place an obligation on industry. Through a sample stocktake of Commonwealth data retention requirements, the Departments identified 739 primary and secondary pieces of legislation when searching 32 terms variously relating to data retention (for example, 'keep records'). Of these, a sample of 209 data retention provisions relating only to industry obligations were analysed by the Departments. This high-level analysis found that some provisions were drafted using more specific language about data retention than others, with some provisions being more ambiguous in relation to retention periods, even for similar data.

Our comments focus on some of the draft data retention Principles (**draft Principles**) proposed in the Discussion Paper, considered through a lens of promoting consistency and harmonisation with the existing regulatory framework, especially the Australian Privacy Principles (**APPs**).

Draft Principle 2 and APP 11.2

In our members' experience, many data retention provisions can make it difficult to apply APP11.2. In our view, draft Principle 2 in the Discussion Paper may be beneficial in situations where the data retention provision does not indicate a clear retention period or when the provision does not indicate the action to be taken after the specified period ends.

Draft Principle 2 states:

> **Agencies should ensure retention provisions have a specified period, including when the retention period begins and when it ends.**

> **Aim**: To minimise the risk of entities retaining information for longer than necessary and provide clarity to regulated entities about their retention obligations.

Under APP 11.1, entities covered under the *Privacy Act 1988* (**APP entities**) are required to take reasonable steps to protect the personal information they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure.[1]

Under APP 11.2, APP entities are also required to take reasonable steps to destroy or de-identify the personal information held once the personal information is no longer needed for any purpose for which the personal information may be used or disclosed under the APPs. This requirement does not apply where the personal information is contained in a Commonwealth record or where the entity is required by law, or a court or tribunal order to retain the personal information.[2]

Generally, this means that APP entities must have in place data destruction policies and procedures while also safeguarding the personal information that they continue to hold from security risks. The guidance from the Office of the Australian Information Commissioner (**OAIC**) does not articulate whether the reasonable steps in APP 11.2 encompass the allocation of retention periods for particular kinds of personal information an APP entity holds. Rather, the OAIC recommends the entity takes into account a range of factors in deciding what the reasonable steps are (such as the amount and sensitivity of the personal information and possible consequences to an individual)[3] and encourages entities to turn their minds to retention obligations as follows:

> However, depending on the type of entity and the type of personal information involved, you may have specific obligations under law or a court/tribunal order to retain and/or destroy or de-identify personal information. Agencies also have specific retention obligations for personal information that forms part of a Commonwealth record.
>
> - Do you have policies, procedures and resources in place to determine whether personal information you hold needs to be: retained under law or a court/tribunal order, destroyed or de-identified?
>
> - Are your staff informed of document destruction procedures?[4]

In our view, the existing OAIC guidance does not provide sufficient clarity on how long personal information should be held after its relevant purpose expires or its legislated retention period ends. As the Discussion

[1] Office of the Australian Information Commissioner, 'Read the Australian Privacy Principles': https://www.oaic.gov.au/privacy/australian-privacy-principles/read-the-australian-privacy-principles.
[2] Office of the Australian Information Commissioner, 'Read the Australian Privacy Principles': https://www.oaic.gov.au/privacy/australian-privacy-principles/read-the-australian-privacy-principles.
[3] See [11.33] of the APP Guidelines.
[4] Office of the Australian Information Commissioner, 'Guide to securing personal information', Part B: https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/guide-to-securing-personal-information#part-b-steps-and-strategies-which-may-be-reasonable-to-take.

Paper notes,[5] the Government has agreed in principle to amend APP 11 to require entities to establish their own maximum and minimum retention periods in relation to the personal information they hold.

In many cases, data retention laws do not provide clarity on these points either. There are a variety of data retention provisions that apply to different industries. Where these provisions state that data must be retained for a specified period but does not provide an end date for retention, there is ambiguity for the entity as to whether data retained beyond the legislated period continues to be held on the basis that it is "required by law".

For example:

- Some provisions create an obligation to make a record but do not specify a retention period: see sections 168 and 169, *Corporations Act 2001*, which requires a register of members (including former members) to be set up and maintained, but does not include a requirement for either the period of retention or the end date for retaining the register.

- Some provisions require a set number of years for retention, and in practice, these provisions are often interpreted as *minimum* retention periods. It is unclear whether an APP entity is permitted to also retain the data for an additional unknown period because of the absence of a clear end date for retention, or provision for deletion or de-identification. See:
  - section 286, *Corporations Act 2001*: "*The financial records must be retained for 7 years after the transactions covered by the records are completed"*.
  - section 4, *Health Insurance Act 1973*: A person who provides a professional service "*must retain the document for the period of 2 years beginning on the day the service is rendered*" in the context of health practitioners claiming Medicare benefits.

In our view, those data retention provisions that do not indicate a clear end date could benefit from draft Principle 2 in the Discussion Paper. It would provide clarity on what a reasonable retention period is under APP 11.2 if the beginning and end of the retention period, as well as deletion requirements in appropriate cases, were specified in the data retention legislation.

Draft Principles 3 and 4

Draft Principle 3 states:

> **Agencies should consider aligning retention periods within the same legislation or policy where possible, noting that each retention provision should be informed by the type, sensitivity and purpose of the data.**

[5] At footnote 6 of page 7 of the Discussion Paper.

> **Aim:** To minimise the risk of entities retaining large volumes of data. The assumption is that entities may seek to simplify and streamline their record-keeping practices by adhering to the longest retention period amongst similar data retention requirements in a given piece of legislation.

Draft Principle 4 states:

> **Agencies should consider the interaction with other legislative requirements to avoid creating duplicating, overlapping or conflicting requirements.**
>
> **Aim:** Considering the interaction with other legislative requirements will help agencies determine if retention is required under the relevant instrument in question, reducing the risk of duplication or overlap which can increase burden and uncertainty for entities.

The alignment of retention periods within the same legislation or policy where possible, and the avoidance of duplication or conflict between legislative requirements, is consistent with our long-standing support for the harmonisation of obligations, which will minimise confusion and increase certainty to foster compliance. On this basis, we support draft principles 3 and 4. In addition to aligning retention periods, we suggest that the nature of the obligations should be consistent.

Some examples can be found in the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* where there is inconsistency in the nature of the retention obligation:

- section 35E: A credit reporting body that receives a verification request in relation to an individual must retain certain information for 7 years after the request was received (s 35E(1)). This retention requirement is accompanied by a clear deletion obligation at subsection 35E(2): *"A credit reporting body that retains information under subsection (1) must delete the information at the end of the 7 year period referred to in that subsection."* Similar obligations are contained in section 35F.
- section 108: The reporting entity must retain customer-provided transaction document, or a copy of the document, for "*7 years after the giving of the document*" (s 108(2)), but there is no requirement for deletion at the end of the 7-year period.

If the draft Principles are implemented in the future and result in changes to data retention provisions, we suggest that guidance and education will assist with compliance. Alignment of retention periods, for example, may allow for the publication of an inventory of data retention obligations across multiple pieces of legislation that apply to the same industry or similar types of data. Examples of regulators providing a summary of obligations include the 'Inventory of super trustee disclosure obligations' published by Australian Securities and Investments Commission[6] and 'Record keeping for business' published by the Australian Taxation Office.[7]

[6] Australian Securities and Investments Commission, 'Inventory of superannuation trustee transparency and disclosure obligations': https://url.au.m.mimecastprotect.com/s/ivKtCXLKNMTnpAnMH6fJTWHpYR?domain=asic.gov.au/.
[7] Australian Taxation Office, 'Index – Record keeping for business': https://www.ato.gov.au/businesses-and-organisations/preparing-lodging-and-paying/record-keeping-for-business/index-record-keeping-for-business.

We understand that the Departments will provide a final report with recommendations and options to "simplify and clarify data retention obligations for industry – with a focus on minimising unnecessary data retention".[8] We look forward to providing more comments on the detailed recommendations of that report when available.

If you have any queries about the items above, or would like further information, please contact Mimi Lee, Policy Lawyer, on 02 9926 0174 or mimi.lee@lawsociety.com.au.

Yours sincerely,

Jennifer Ball

Jennifer Ball
President

[8] Page 3 of the Discussion Paper.