

14 September 2026

Our ref: KS:PDTIP

Dr James Popple
Chief Executive Officer
Law Council of Australia
Level 1, MODE 3
24 Lonsdale Street
Braddon ACT 2612

By email: [REDACTED]

Dear Dr Popple

Privacy Amendment (Personal Data Protection) Bill 2026 and related reform proposals

Thank you for the opportunity to provide feedback on the *Privacy Amendment (Personal Data Protection) Bill 2026 (the draft Bill)* and related reform proposals in the Privacy Reform – Consultation Paper (**the Consultation Paper**).

This response was informed by members of our Privacy, Data, Technology and Intellectual Property Law Committee whose members have expertise in this area. In the time available, members raise the following concerns with the draft Bill.

Definitions

QLS supports the amendment to the definition of personal information to cover information that '*relates to*' an identified individual, or an individual who is reasonably identifiable. The Privacy Act Review report¹ highlighted that the definition should be supported by explanatory materials and OAIC guidance.

The example provided on page 5 of the Consultation Paper is insufficient to clarify the policy intention, that is, that the connection between the information and the individual is not too tenuous or remote.

We recommend an additional note be included in the legislative drafting to clarify what '*relates to*' means. This should be supplemented by additional examples in the Explanatory Memoranda. The OAIC will also need to prepare guidance on this matter.

¹ https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf.

With regard to the 'fair and reasonable test' in the context of handling personal information, members generally consider the drafting is workable but that additional guidance is needed, particularly with respect to the excepted 'permitted general situations'.

With regard to the new definition of 'discloses', members welcome the definition but consider guidance is needed as to the intended meaning of 'accessible to' [another person or body], particularly given this definition changes earlier and consistent regulatory guidance in the context of outsourced service providers and cloud services (which allowed for a distinction between 'use' and 'disclosure' where effective control was retained over the handling of the personal information). We discuss further implications within the context of the new 'controller' and 'processor' provisions, and overseas disclosures, below.

Retrospectivity

It is of note that many of the amendments would apply, whether the information was acquired or created before, on or after the commencement of the draft Bill.² Laws that change legal rights and obligations with retrospective application undermine the rule of law and can cause significant practical difficulties.

Given the broad assessment required of personal information already held by organisations, including to ensure that personal information is de-identified, having regard to the particular context (and a potentially broader scope of personal information that 'relates to' an individual), and the shifting of responsibilities between controllers and processors, QLS strongly recommends a reasonable transition period be applied to allow businesses to prepare for commencement and support their compliance.

Processors and Controllers

The draft Bill seeks to introduce concepts of, and allocate responsibility between, personal information controllers and processors.

Australia's population has reached approximately 27.8 million³, making domestic customer reach a focus for many Australian businesses. Further, a vast majority of these businesses rely on third-party service providers and cloud platforms to collect, process, and manage personal information.

It is therefore difficult to reconcile any public benefit in substantially increasing those businesses' privacy law obligations while simultaneously decreasing the privacy law rules applying to those they materially rely on to comply with those obligations. This is especially the case given that the terms offered by service providers are often unclear or ambiguous, complex, may be unilaterally updated, and not realistically negotiable.

While Committee members considered there would be benefit in reducing privacy law compliance obligations on service providers who do not have any meaningful independence

² For example to:

- the definitions of *collects*; *de-identified*; *health information*; *personal information* and *sensitive information* (s 6)
- the meaning of *trade* (s 6FC)
- the replacement of APPs 3 – 5 and 11 and the amendments to APP 12,

as per the following draft Bill Schedule 1 s 13; Schedule 2 s 28; Schedule 3 Part 2 and Schedule 4 Part 1.

³ [Population | Australian Bureau of Statistics](#).

Privacy Amendment (Personal Data Protection) Bill 2026 and related reform proposals

as regards the personal information they manage for others, QLS considers the current proposal in the draft Bill does not achieve a practical balance in allocating responsibilities between entities.

The *partial* adoption of these concepts from overseas data protection regimes (most notably the EU General Data Protection Regulation (**GDPR**) but also present in other jurisdictions), in the draft Bill will be onerous for Australian businesses, and risks creating further complexity and disputes, with no clear benefit for consumers.

We acknowledge the distinction exists between controllers and processors in the GDPR.^[1] However, this distinction is supported by broader regulatory frameworks and requirements to assist regulated entities to comply with their respective obligations. The proposed exceptions for processors from APP compliance (other than APPs 1 and 11) in ss 6A(2A) and 6B(2A) of the draft Bill, without broader reforms to the *Privacy Act 1988* (Cth) (**Privacy Act**), do not sufficiently reflect key aspects of the GDPR nor the current ecosystem for businesses captured as “controllers”.

For example, the GDPR provides for joint and independent controllership, and that controllers and processors may be liable to fines and other penalties under the GDPR.^[2] There are also clear delineations between the responsibilities and liabilities of controllers and processors including in the context of a personal data breach.

Under the draft Bill, where a processor acts in accordance with a controller's documented instructions, the processor's acts are taken to be acts of the controller. This is in the context of no legislative or other guidance as to instructions which should be issued by the controller and contrasts with Article 28 of the GDPR which sets out several matters which should be governed by a contract or other legal act, binding on the processor, regarding the controller and under which recognised “Standard Contractual Clauses” (**SCCs**) provide welcome clarification for controllers.

There is also no proposed carry-through of these concepts under the draft Bill to data breach response, assessment and notification obligations under the Notifiable Data Breaches scheme.

Some possible solutions:

“Controllers”

Section 16D of the draft Bill suggests that a “controller” is any counterparty to a service provider for whom the service provider does an act or engages in a practice. This definition is too broad and does not have regard to the fact that counterparties to service provider contracts may not themselves determine the means and purposes of processing by the service provider. This aspect should be clarified.

“Processors”

Characterisation: The characterisation of an entity as a processor for the purpose of s 16D may be easily orchestrated by contract terms designed to satisfy the elements of section

^[1] Chapter 4 (Art. 24-43), [Chapter 4 – Controller and processor - General Data Protection Regulation \(GDPR\)](#).

^[2] [Controller and Processor relationships | Data Protection Commission](#)

16D(1) without regard to the substance of the relevant arrangement. For example, it is not uncommon for cloud or other service contracts involving personal information to provide that the service provider may use and disclose personal information disclosed to or 'made accessible to' it for ambiguously stated purposes, for example "*service improvements*" or for its own data analytics and commercial purposes and benefit.

If, however, the contract with the service provider gives the service provider permissions to do this and states that, when doing so, the service provider is acting in accordance with the contract terms, the service provider may have the benefit of the ss 6A(2A) and 6B(2A) *Privacy Act* defences in circumstances where the purposes are, in commercial substance, the service provider's purposes rather than those of the counterparty. The contract terms will often also require the customer to provide warranties and/or indemnities for the benefit of the service provider with respect to the handling of the personal information in connection with the services.

There should be a legislative direction that the ss 6A(2A) and 6B(2A) defences (and, conversely, the counterparty's vicarious liability under s 16D(2)), should be determined by substance, not form.

Model processor clauses: There should be a legislative requirement for model processor clauses such as the SCCs. Promulgation of these would give certainty to Australian businesses in relation to personal information flows to their service providers and maintain the rights of individuals to seek access to and correction of personal information processed by the processor.

Related to this, the ss 6A(2A) and 6B(2A) defences should only be available to processors if they establish that there is no breach of those SCCs. Conversely, the counterparty's vicarious liability under s 16D(2) of the draft Bill should apply where the counterparty has done what it is reasonably able to ensure compliance with the SCCs.

Pre-conditions to processor defences: Given that the terms offered by many service providers are often unclear, the ss 6A(2A) and 6B(2A) defences should only be available to processors if:

- they establish that they have done all that is reasonably appropriate to provide sufficient information to their counterparties to enable their counterparties to comply with the APPs; and
- prior to entering into their contract with their counterparties, they have given their counterparties a clear, current and unambiguous summary of the uses, disclosures and purposes to which their management of personal information accessed under the contract will and will not be limited, in a form suitable for the counterparties to provide to individuals whose personal information is to be disclosed under the contract.

Sub-processors

QLS suggests that determining whether an entity is, for s 6EB of the draft Bill and APP 14 purposes, a "large digital platform", should take into account sub-processors (acting on instructions and on behalf of a processor).

Section 5B and APP 8 (Cross-border disclosure of personal information)

Privacy Amendment (Personal Data Protection) Bill 2026 and related reform proposals

Section 5B(3): Section 5B(3) should be supplemented to provide that an organisation or small business operator should also be deemed to have an Australian link if it is not as described in ss 5B(2) or 5B(3), but processes personal information for an organisation or small business operator whom it should reasonably know has the requisite Australian link. This amendment would give Australian businesses some reasonable basis for a belief referred to in APP 8.2, and otherwise ensure that Privacy Act obligations on those who “hold” personal information extend to those whose role may only be that of a processor to an APP entity.⁴

APP 8.3: The new definition of “discloses” would increase compliance burdens on Australian businesses who give access to ex-Australian entities [see earlier discussion].

To provide certainty to Australian businesses, legislative reform should be accompanied by regulations which clearly designate the laws of countries for the purpose of APP 8.3, as it relates to disclosure of personal information by an APP entity to an overseas recipient.

Joint and independent “controllers”

GDPR Article 26 recognises that two or more controllers may determine the purpose and means of processing as “joint controllers”. It also recognises circumstances in which a service provider may be both a processor and an independent controller. These concepts are overlooked in the draft Bill. Section 16D presents a binary view – an entity is either a “processor” or a “controller”. In reality, an entity may be both. This aspect should be clarified and appropriate provisions included in the draft Bill to ensure appropriate allocation of accountability and liability for compliance with the Australian Privacy Principles (APPs).

APP carveouts

QLS does not consider that, even where a service provider is acting without any substantive means to determine the means and purposes of processing of personal information, but nevertheless is in possession or control of that personal information,⁵ there is sufficient justification for exonerating processors from the following APPs:

- *APP 3.1 (fairness, reasonableness and lawfulness).* APP 3.2 could be supplemented to provide that whether an APP entity is a processor, and if so the relevant contract terms, are relevant considerations;
- *APP 4.2 (no trade in personal information without consent);*
- *APP 5.1 (awareness),* unless the processor has taken reasonable steps to satisfy itself of its counterparty's APP 5.1 compliance;
- *APP 7.1 (no direct marketing)* unless the processor has taken reasonable steps to satisfy itself of APP 7 compliance by its counterparty;
- *APP 10 (quality of personal information).* APP 10 could be supplemented to provide that whether steps are “reasonable in the circumstances” could have regard to whether the APP entity is a processor only in respect of the relevant personal information;
- *APP 11 (security and destruction of personal information).* APP 11 could be supplemented to provide that what steps are “reasonable in the circumstances” could have regard to whether the APP entity is a processor only in respect of the relevant personal information;

⁴ Noting that there is no proposal to change the s 6 definition of ‘holds’ (that “an entity holds personal information if the entity has possession or control of a record that contains the personal information.”)

⁵ Namely, “holds” it.

- *APP 12 (access to personal information)*. APP 12 could be supplemented to provide, in APP 12.3, that access is not required of the processor where the access is available from the controller and the processor provides the requestor with the controller's details and acts reasonably to assist the controller in acceding to the request. APP 12.3A of the draft Bill could be supplemented to provide that a controller is not required to give access to the extent it has not been given reasonable assistance from the processor regarding the access request.

Supporting compliance with guidance and information

Captured businesses should be supported to uplift their compliance with the Privacy Act as amended by the draft Bill prior to commencement.

Review of OAIC Guidance and input from stakeholders including small business and legal stakeholders will be critical, together with further guidance in the Explanatory Memorandum to the draft Bill.

Members support the following provisions of the draft Bill but consider that further guidance and awareness raising from the OAIC is necessary for practical implementation:

- Information about geolocation tracking data in the context of its inclusion as "sensitive information" and its cumulative nature i.e. that it is collected and held over time. That is, what this means in a practical, consumer and customer facing circumstance. Regulator guidance will also be needed as to what the new requirements for consent will practically look like for geolocation data.

For example, many Software as a Service (**SaaS**) providers collect and process geolocation tracking data without knowledge to the businesses using their services. Further, they often embed third party tracking pixels, diagnostic tools or performance monitors that automatically capture IP addresses and location data during general use. Geolocation data can therefore be layered amongst several providers.

Members suggest that the requisite level of understanding of these features are not readily understood by businesses or consumers so there will be a level of education required to support compliance with this reform.

- Changes to the definition of consent and clarity/pathways for businesses in unequal bargaining positions negotiating service provider terms.
- Clarity for businesses who may incidentally "trade" in personal information given the definition is intended to cover a broad range of arrangements.
- Supporting small businesses with the eligible data breach 72-hour notification period. While we support this approach, the reality is that many small businesses will still struggle to meet this and should be supported with a targeted pathway for small business. Members consider this will also mitigate over-notification to the OAIC and/or interim notifications under the new s26WK(7) that are not meaningful or required. Regulatory action should be targeted towards supporting businesses. It would also be

Privacy Amendment (Personal Data Protection) Bill 2026 and related reform proposals

helpful for regulated entities to have practical guidance on the application of remedial actions described in ss26WL(6) and (7).

Businesses who are not APP entities or who may have some APP compliance obligations with respect to some personal information held should still be supported with privacy aware information and guidance.

OAIC's guidance documents are of great importance to Australian businesses in how they practically navigate the complexities of the Privacy Act. QLS does not support the amendments to s92 of the Privacy Act which would remove Administrative Review Tribunal review of decisions of the Commissioner regarding guidelines (refusing to approve the issue; refusing to approve and revoking approval).

Related reform proposals

Employee record exemption

QLS notes removal of the employee exemption has not been addressed by the draft Bill. The Society has previously submitted that the exemption should be removed. There are practical challenges for businesses by its continued operation and the duality of dealing with some information in different ways. We understand the reality is that the exemption is generally being applied in the narrowest sense in APP organisations, in any event, given case law, regulatory guidance and confidentiality concerns. It makes most sense for organisations to simply treat all employee information as protected.

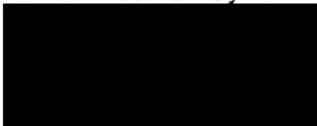
Financial abuse

QLS has previously raised that privacy issues in the financial services sector can impede the ability for victims and their advisors to deal with issues of financial abuse, including elder financial abuse. We have suggested that limited exceptions to privacy protections should be considered in this context.

In this regard, we have had the benefit of reviewing the submission of the Queensland Public Advocate to this consultation and endorse consideration of Dr Chesterman's recommendation in respect of "the introduction of an additional category of 'permitted general situation' (s. 16A), which could draw on existing terminology utilised by the Royal Commission into Violence, Abuse, Neglect and Exploitation of People with Disability and define 'safety' in s. 16A to mean 'freedom from violence, abuse, neglect or exploitation, including financial abuse or exploitation'".

If you have any queries regarding the contents of this letter, please do not hesitate to contact our Legal Policy team via policy@qls.com.au or by phone on [REDACTED] [REDACTED]

Yours faithfully



Peter Jolly
President