Law Council
OF AUSTRALIA

21 September 2026

Privacy Reform Team
Attorney-General's Department
Robert Garran Offices
3–5 National Circuit
BARTON ACT 2600

By email: PrivacyReform@ag.gov.au

Dear Privacy Reform team

Privacy Amendment (Personal Data Protection) Bill 2026

1. The Law Council of Australia welcomes the opportunity to provide a submission to the Attorney-General's Department in response to the exposure draft *Privacy Amendment (Personal Data Protection) Bill 2026* (the **Bill**) and accompanying *Privacy Reform Consultation Paper* (the **Consultation Paper**).

2. The Law Council thanks the Law Society of New South Wales; the Queensland Law Society; the Law Institute of Victoria; the Victorian Bar; the Law Society of Western Australia; and the Privacy Law Committee of its Business Law Section for their contributions to the preparation of this submission.

Consultation process

3. The Law Council appreciates the release of the Bill, as it is important that exposure draft legislation is publicly released. However, it remains concerned by the limited timeframe for consultation on the Bill. The consultation opened on 31 August 2026 and closes on 18 September 2026, providing fewer than three weeks to consider the Bill and Consultation Paper. In addition, the Bill does not contain all the provisions contemplated as part of the reform package and the consultation materials do not include an exposure draft Explanatory Memorandum. We further note the Consultation Hub indicates that late submissions will not be considered.[1] We hope that this (slightly) late submission will be considered.

4. Given the breadth, significance and technical complexity of the reforms, this timeframe is insufficient for detailed consideration of their legal and practical implications. These constraints are compounded by the request that submissions be limited to approximately 1000 words. Unfortunately, we were unable to meet this requirement.

---

[1] Australian Government Attorney-General's Department, Privacy Reform – Consultation on Exposure Draft legislation (Webpage, 31 August 2026).

Telephone +61 2 6246 3788 • *Email* mail@lawcouncil.au
PO Box 5350, Braddon ACT 2612 • Level 1, MODE3, 24 Lonsdale Street, Braddon ACT 2612
Law Council of Australia Limited ABN 85 005 260 622
www.lawcouncil.au

5. As a membership-based peak organisation, the Law Council consults its constituent bodies, sections and advisory committees in developing law reform positions. The limited timeframe has substantially constrained this process. Accordingly, the views expressed in this submission are necessarily preliminary and should not be taken to identify all issues arising from the Bill.

6. The Law Council acknowledges the extensive consultation undertaken through the Privacy Act Review and subsequent reforms. However, consultation on earlier policy proposals is not a substitute for adequate scrutiny of the legislative provisions intended to implement them, particularly where the Exposure Draft contains measures that were not previously consulted upon or differ from earlier proposals. The Law Council has consistently emphasised that adequate consultation supports high-quality lawmaking and reduces the risk of unintended consequences.

7. We note that the Office of Impact Analysis' Best Practice Consultation guidance previously indicated that 30 to 60 days was usually appropriate for effective consultation.[2] While we acknowledge that the Australian Government Impact Analysis Framework changed from 1 July 2026, consultation should remain proportionate to the significance and complexity of the proposed regulatory change. The present timeframe does not, in the Law Council's view, meet that standard. The Government should undertake further targeted consultation on revised and additional draft provisions before the Bill is introduced into Parliament.

Overarching comments

8. A number of the proposed amendments would apply to personal information held after commencement, irrespective of whether that information was acquired or created before the new measures take effect. While this approach promotes consistency in the treatment of personal information, it creates significant implementation challenges for APP entities, particularly where existing systems and information holdings were established by reference to the current requirements of the Privacy Act.

9. Given the breadth of the proposed reforms and their operational implications, the Law Council recommends that an appropriate transition period be provided to enable APP entities to prepare for commencement and support their effective compliance. The appropriate period should have regard to the nature and complexity of the particular obligations and any changes to systems, processes and contractual arrangements required to implement them: a period of at least two years has been suggested.

10. Throughout the Bill, there are several issues that require further guidance to support compliance, including resolution of ambiguities within the text of the legislation, and where appropriate, further explanation in the Explanatory Memorandum and in guidance materials developed by the Office of the Australian Information Commissioner (**OAIC**). The OAIC must be adequately resourced to ensure that this guidance material can be developed and provided in a timely manner, and through a process that involves adequate stakeholder consultation.

---

[2] Office of Impact Analysis, Best Practice Consultation (Guidance Note, July 2023) 7.

11. The Law Council also notes that the Children's Online Privacy Code is being finalised concurrently with the present reforms. The Government and OAIC should ensure that the final Code and the amendments proposed by the Bill are appropriately aligned, including in relation to their commencement and implementation.

Schedule 1—Core definitions

Definition of personal information

12. The Bill proposes to insert a new definition of "personal information" in section 6FD.[3] The definition is framed as information or an opinion that "*relates to*" an identified or reasonably identifiable individual, as opposed to "*about*" an individual as "personal information" is currently defined at subsection 6(1) of the *Privacy Act 1988* (Cth).

13. The Law Council has previously expressed in-principle support for proposals directed to clarifying the definition of personal information, including recognition of inferred and generated information and greater clarity concerning reasonable identifiability.[4]

14. We note that, in proposing the change from "*about*" to "*relates to*", Proposal 4.1 of the Privacy Act Review Report further specified that the definition be appropriately confined to where the connection between the information and the individual is not too tenuous or remote, through drafting of the provision, explanatory materials and OAIC guidance.[5] We also observe the definition of sensitive information has retained the reference to being 'about' an individual's characteristics as listed. Further clarity will be required to delineate the distinctions, if any, between the degree of connection required for information to be 'related' to an individual to meet the definition of personal information as defined and to be 'about' an individual's protected characteristic as listed in subsection 6FE(a) as proposed.[6]

15. On its face, the proposed provisions of the Bill do not expressly articulate the degree of connection required between information and the individual for information to "relate to" that individual, and the term is not further defined. The Consultation Paper indicates that "relates to" in and of itself signifies the degree of connection required, in that bearing its ordinary meaning "there must be a sufficient connection" between the information and the individual in the circumstances.[7]

16. Furthermore, the example provided in the Consultation Paper indicates that whether information relates to an individual may change according to the purpose for which the information is handled.[8] Information that is not personal information when initially created or collected may therefore subsequently become personal information because of a new use. We note that, while this may be appropriate in principle, it creates practical questions about when obligations under the Privacy Act would attach to information already held by an entity.

---

3 Privacy Amendment (Personal Data Protection) Bill 2026, Schedule 1, Item 12, s 6FD.
4 Law Council of Australia, *Government Response to the Privacy Act Review Report* (Submission, 13 April 2023) [35]–[36].
5 Australian Government Attorney-General's Department, *Privacy Act Review* (Report, 2022) 27, Proposal 4.1 ('Privacy Act Review').
6 Privacy Amendment (Personal Data Protection) Bill 2026, Schedule 1, Item 12, s 6FE.
7 Australian Government Attorney-General's Department, *Privacy Reform* (Consultation Paper, 2026) ('Consultation Paper') 4–5.
8 Ibid.

17. We have also previously conveyed concerns from some of our stakeholders about the risks of significantly expanding the scope of information that falls within the definition of "personal information". The concern is that this may result in trivial or innocuous information being subject to the protections under the Act, attracting a disproportionately large compliance burden.[9] We note that these concerns persist with respect to proposed amendments to personal information under the Bill, including the change from "*about*" to "*relates to*".

18. Our feedback indicates that Note 1 to proposed section 6FD may create uncertainty as to whether the concepts of identification and reasonable identifiability extend to circumstances in which an individual can be "singled out" or otherwise dealt with as a "distinct individual", notwithstanding that their identity cannot be ascertained.

19. This raises questions concerning the distinction between identification and "individuation", the latter of which the Privacy Act Review considered should remain outside the definition of "personal information" and instead be addressed in relation to targeting.[10] The intended operation of Note 1 should therefore be clarified, including whether the ability to single out or distinguish an individual, without the capacity to ascertain that individual's identity through information reasonably available, is intended of itself to satisfy the requirement that an individual be "identified" or "reasonably identifiable".

Collection of personal information

20. There is general practitioner support for the amendment to the definition of "collects". Some feedback has expressed the view that the wording of the Note to proposed section 6AAA should be expanded to read "deriving, inferring or deducing it from other information" (proposed amendment underlined). It has been further suggested that there be consideration of recent determinations of the Privacy Commissioner[11] with respect to when an entity will be taken to have collected personal information, and whether the Bill provides an opportunity to clarify these positions.

Disclosure of personal information

21. The Law Council has received mixed feedback on the proposed amendments to the definition of disclosure, which would clarify that disclosure occurs when personal information is made accessible to another person or body. While feedback in support of the proposed amendments calls for greater guidance material, others raise significant concerns that the proposed definition does not align with how processes operate in practice, particularly with respect to overseas storage of data, such as occurs in the provision of cloud computing services, which is currently considered to be a "use" of the information, not a "disclosure".

22. We understand from the Consultation Paper[12] that the proposed amendments to the definition are not intended to cut across this current understanding. However, in

---

9 Law Council of Australia, *Government Response to the Privacy Act Review Report* (Submission, 13 April 2023) [34].

10 Privacy Act Review (n 5) 35 – 36.

11 *Commissioner Initiated Investigation into Monash IVF Pty Ltd (Privacy*) [2026] AICmr 40 and *Commissioner Initiated Investigation into Medmate Australia Pty Ltd (Privacy)* [2026] AICmr 41.

12 Consultation Paper (n 7) 8.

practice, cloud computing contracts generally permit a level of access to the information stored by the cloud service provider. While that access should be strictly limited, it is typically necessary to address support requests, technical issues, or enable the cloud service provider to implement effective security measures. It is recommended that this issue be clarified, ideally within the primary legislation.

Schedule 2—Handling personal information

Part 1—Fair and reasonable handling of personal information, consent and notice requirements

23. The Law Council has previously expressed in-principle support for the introduction of an overarching fair and reasonable test. With any new legislative test, there is a focus on potential uncertainty and, in this instance, we are of the view that targeted revisions to the Bill and additional guidance will be necessary to improve certainty for APP entities seeking to comply with the new framework.

24. Suggestions to support introduction and address the risk-based nature of the test include:

- providing a list of factors (which may be non-exhaustive) that the test is intended to capture (or preferably, with the addition of a "safe harbour" a presumption of fair and reasonable handling where certain factors are met);
- clarifying the concept of "genuine choice"[13] and how it differs from "consent";
- clarifying how transparency failures interact with the fair and reasonable test as well as further consideration as to whether transparency should operate as a standalone consideration;
- providing clarity that an appropriate review process by the APP entity would address the requirements;
- providing further guidance with respect to excepted "permitted general situations"; and
- providing additional guidance on data minimisation.

25. We also note that the concepts of "reasonably necessary" and "primary/secondary purpose" under the existing Privacy Act framework are well understood, and query whether they could be retained in support of the new fair and reasonable test, such as via express reflection in the legislative factors. These factors could be valuable touchstones to guide implementation of the new test. It is unclear from the consultation materials why the existing language could not be retained in an appropriate form.

26. It has also been suggested that the new fair and reasonable test may result in practice in APP entities needing to undertake (and regularly review) privacy impact assessments for all collections, uses and disclosures, regardless of the level of risk. If that is the underlying intention, that should be explicit in the text.

27. The Law Council notes that proposed APP 3.2(b) refers to whether the collection, use or disclosure of information "relates to" one or more of the APP entity's functions or

[13] Privacy Amendment (Personal Data Protection) Bill 2026, Schedule 2, Part 1, Item 10, APP 3.2(e).

activities, with the Consultation Paper stating that this requires "a clear connection".[14] This contrasts with the meaning ascribed to "relates to" in the Consultation Paper with respect to "personal information", which requires a "sufficient connection", implying that differing interpretations may be applied to the same term across the Bill.

Part 2—Permitted general situations

28. The proposed amendment to Permitted General Situation (**PGS**) item 2 would change "*misconduct* of a serious nature" to "*wrongdoing* of a serious nature" (emphasis added).[15] The Consultation Paper explains that this is intended to be "broader than misconduct" and may include conduct by a person acting in a private capacity, such as in cases where an entity suspects a customer may be experiencing financial abuse.[16]

29. While the Privacy Act currently defines "misconduct" at subsection 6(1), "wrongdoing" is not defined, and no proposed definition is included in the Bill. Given the breadth of conduct potentially encompassed by the expression, the Law Council considers that greater certainty should be provided as to its intended scope including defining "wrongdoing" in the legislation, rather than relying on examples in extrinsic material or subsequent regulatory guidance.

30. The PGS in items 4 and 5 have been drafted to permit disclosures where it is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim[17] or for the purposes of a confidential alternative dispute resolution process[18] but only where disclosure is *not* to an overseas recipient. This seems to preclude such disclosure in the case of disputes outside Australia.

31. The Consultation Paper does not explain why disclosures in PGS items 4 and 5 should be excluded merely because the recipient is overseas. In practice, legal claims and dispute resolution processes may involve holding companies, subsidiaries, overseas courts, tribunals, arbitral bodies, counterparties, witnesses, experts, insurers, underwriters, or legal advisers. Excluding overseas recipients may create uncertainty and impede the effective conduct of cross-border litigation and dispute resolution, including where overseas disclosure is necessary for the legal claim or dispute resolution process, and where appropriate professional, contractual or procedural safeguards are in place.

32. Provided the information is handled in compliance with the Privacy Act and relevant rules, this would disproportionately disadvantage parties to disputes with a global or cross-border element. This appears to be an unintended consequence and can be addressed in the Bill by expressly dealing with disclosures to overseas recipients. The Law Council recommends that the Government explain the policy rationale for this distinction and consider whether items 4 and 5 should be amended to preserve the existing position, or otherwise clarify the circumstances in which overseas disclosures for legal claims and confidential dispute resolution may occur.

---

[14] Consultation Paper (n 7) 12.
[15] Privacy Amendment (Personal Data Protection) Bill 2026, Schedule 2, Part 1, Item 17, ss 16A(1), PGS 2.
[16] Consultation Paper (n 7) 19.
[17] Privacy Amendment (Personal Data Protection) Bill 2026, Schedule 2, Part 1, Item 17, ss 16A(1), PGS 4.
[18] Ibid, PGS 5.

Part 3—Direct marketing

33. The Law Council has received mixed feedback in relation to the changes to APP 7. Some broadly welcome the underlying intent of the amendments and increased obligations on organisations to fulfil the request of the person seeking to 'opt-out' of direct marketing, as compared to the current framework. However, it has been queried whether there is sufficient rigour in the framework for an individual opting-out of direct marketing or communications without further guidance as to what constitutes *"such steps as are reasonable in the circumstances to give effect to the request"*[19] given the wide discretion of what might be considered *"reasonable"* and noting that the Consultation Paper acknowledges that reasonable steps may depend on factors of the entity.[20]

34. Other feedback has sought additional clarity on the requirements under APP 7, noting that the breadth of the new definition of direct marketing[21] introduces new concepts such as an individual being 'a member of a class' and a concept of "identification or other targeting is done using personal information *that relates to the individual"* (emphasis added). We query the meaning of the additional reference to relating to the individual, noting that the concept of 'relates to' is already a threshold issue of what amounts to personal information as defined in proposed section 6FD.

35. Consideration should be given to the interaction between the proposed definitions of "trading" in section 6FC and "direct marketing" in subsection 6(1). In this regard, the definition of "trading" may capture the sharing of technical identifiers, such as cookies or device identifiers, between entities for the purpose of facilitating direct marketing. While such practices may give rise to privacy risks, their nature and extent will depend on the information shared, the purposes for which it is used and the extent to which it enables individuals to be identified, tracked or profiled. There should be further consideration as to whether the interaction between the proposed trading and direct marketing provisions appropriately accounts for these differences, including the implications for online publishers that rely on third-party advertising services.

36. Further consideration should also be given to the practicality of compliance and implementation with new APP 7.3, which requires a direct marketing communication to be accompanied by information on how to opt-out, in the context of web-delivered direct marketing (such as advertising collateral served on a webpage). This should clarify the role and scope of website operators in managing marketing opt-outs, and be supported by practical implementation guidance.

---

[19] Privacy Amendment (Personal Data Protection) Bill 2026, Schedule 3, Part 1, item 27, APP 7.2
[20] Consultation Paper (n 7) 20–21.
[21] Privacy Amendment (Personal Data Protection) Bill 2026, Schedule 3, Part 1, item 25, s 6.1.

Schedule 3—Data security

Part 1—Notifiable data breaches

37. The Law Council supports the intent of amendments to provide for an express positive obligation to mitigate potential harms arising from actual or suspected data breaches.[22] However, this must be supplemented by comprehensive and timely guidance, including linking these new obligations with the general obligations under proposed APP 11.5 for ongoing evaluation of the effectiveness of measures to protect information. Guidance materials should also include how compliance with these requirements can be achieved in practice.

38. The Law Council has received mixed feedback about the changes to the notification requirements as proposed in the Bill under proposed section 26WK. While welcomed by some, there are concerns this may create additional complexity and uncertainty and may detract focus from response and recovery efforts to compliance with notification obligations. Again, additional guidance materials will be necessary to support compliance with these requirements. This may include further detail on the expectations around information to be provided under notices, particularly the level of detail required to be provided in the 'statement of reasons' required to support an incomplete statement. Further, to support entities to better understand where reasonable grounds to *suspect* there has been an eligible data breach crystallises into a *belief* there has been an eligible data breach. The introduction of a fixed 72-hour notification period increases the practical significance of distinguishing between these thresholds.

Part 2—Security of personal information

39. The proposed new wording in APP 11 introduces several new concepts that require clarity. For example, we draw attention to the reference to '*any'* steps in the new APP 11.4.[23] This is potentially a very broad and ambiguous reference to steps that may be required and departs from the notion of "reasonable steps" that are the cornerstone security requirements in current APP 11. This is an unintended consequence and must be addressed. We recommend that it be qualified as per other references to read 'any reasonable steps' or a similar qualification to help to address certainty.

Schedule 4—Data access and erasure

Part 1—Technically impossible or infeasible

40. Proposed amendments to APP 12 would insert a new exception to the requirement to give access to personal information where, despite taking reasonable steps to give access to personal information, providing access remains unreasonable or impracticable due to technical impossibility or infeasibility.

---

[22] Privacy Amendment (Personal Data Protection) Bill 2026, Schedule 3, Part 1, item 7, s 26WDA and s 26WDB.

[23] Ibid, Schedule 3, Part 2, Item 22, APP 11.4(b).

41. We note that "technical impossibility or infeasibility" is presented as the same compound phrase in the draft provisions and the limited explanatory material, which does not disclose whether "technically" is intended to qualify "infeasible" as well as "impossible". Further, there is difficulty assessing which of the Macquarie Dictionary senses of "technically" is intended to be applied, and understanding whether some sense of technological impossibility was intended. We observe that this provision seems to be the response to the *Privacy Commissioner v Telstra Corporation Ltd*[24] decision, which has prompted the change to the foundational definition of personal information, and if that is so, it should be mentioned in the explanatory materials.

42. It will be important for the modified data access framework to be supported by guidance on how APP entities should assess, process and refuse requests, including the level of detail required in notices of decision. In practice, the amendments may create a freedom of information (**FOI**)-style review process, without the established framework of the FOI regime. This may create significant compliance challenges, particularly for smaller organisations with limited experience managing data access requests. Guidance should address data access, including prescribing processing time limits and criteria for determining when requests are unreasonable, and establishing regulated processing charges.

Part 2—Right to erasure on large platforms

43. The Law Council supports in principle the proposed introduction of a right for individuals to request the erasure of personal information with an exception where compliance is technically impossible or infeasible. However, we query several elements of the scope of these provisions.

44. There does not appear to be a clear practical or principled justification for why the protection will apply only to "large digital platforms" as defined in the Bill and organisations prescribed by the regulations.[25] Limiting the right to erasure on the basis of an organisation being deemed to be a "large digital platform" despite the significant amounts of personal information being held and privacy risks presented across some other APP organisations would create different regimes for destroying personal information on the basis of the identity and characteristics of the entity holding the information, rather than a consideration of the nature and volume of information held by an entity.

45. Importantly, the Law Council has previously noted that any right to erasure requires careful consideration and detailed consultation with a broad cross-section of stakeholders, not least because there may be numerous unintended consequences. In this regard, we note that the definition of "large digital platforms" under proposed section 6EB[26] includes "designated internet service" within the meaning of the *Online Safety Act 2021* (Cth) as part of the definition. This has the potential to capture a much broader range of APP entities than those indicated in the Consultation Paper[27] but could also extend, for example, to large online retailers or banks. We think that this is an unintended consequence and should be addressed.

---

[24] *Privacy Commissioner v Telstra Corporation Ltd* (2017) 249 FCR 24.
[25] Privacy Amendment (Personal Data Protection) Bill 2026, Schedule 4, Part 2, item 6, s 6EB.
[26] Ibid, s 6EB(1)(a).
[27] Consultation Paper (n 7) 33.

46. We further note that, as currently drafted, the exceptions to the requirement to destroy personal information under proposed APP 14[28] do not include an exception for public interest, scientific, historical or statistical research purposes or exercising the right of freedom of expression and information, as contained in the equivalent European General Data Protection Regulation (**GDPR**) right to erasure.[29]

47. There may be legitimate reasons for an APP entity to retain personal information in circumstances that do not currently appear to be accommodated by the permitted general situations or the exceptions in proposed APPs 14.2 and 14.3. Consideration should therefore be given to whether the proposed exceptions are sufficiently comprehensive to accommodate circumstances in which retention of personal information is reasonably necessary and appropriate, having regard to the rights and legitimate interests of the individual, the APP entity and relevant third parties.

48. These issues raise a broader question as to whether the proposed definition is appropriately calibrated to the privacy risks at which the new right is directed. The Government should explain the basis upon which the relevant service categories and thresholds were selected and demonstrate that they provide an appropriately targeted and proportionate proxy for those risks.

49. Implementation should be further supported by consideration of staged implementation (starting with large digital platforms, as proposed), clarity in the Bill on how the proposed exceptions to this new APP would apply, and the operation of this right in the context of the fair and reasonable test.

Schedule 6—Exceptions for information processors

50. The Law Council has significant concerns about the proposed distinction between controllers and processors, and submits that the Bill in its present form does not achieve a practical balance in allocating responsibilities. Compliance will be onerous for Australian businesses, and risks creating further complexity and disputes, with unclear benefits for consumers.

51. We observe that many 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.

---

[28] Privacy Amendment (Personal Data Protection) Bill 2026, Schedule 4, Part 2, item 11, APP 14.2–14.3.

[29] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* (2016) OJ L 119/1 ('GDPR'), Article 17(3)(a) and (d).

52. We acknowledge the distinction that exists between controllers and processors in the GDPR.[30] However, this distinction is supported by broader regulatory frameworks, a broad concept of processing,[31] and many other 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 sections 6A(2A) and 6B(2A) of the draft Bill, without broader reforms to the Privacy Act, do not sufficiently reflect key aspects of the GDPR nor the current ecosystem for businesses captured as "controllers".

OAIC powers and efficiency measures

53. The Consultation Paper flags several proposed measures not contained in the exposure draft relating to the OAIC's powers and efficiency. Without the benefit of seeing how these measures would appear in legislative form, we note the following observations against two areas of proposed change.

Dispute resolution requirements

54. The Law Council recognises the benefits of resolving privacy complaints at the earliest appropriate stage and considers it reasonable, in principle, for individuals to first raise complaints directly with the relevant APP entity. However, the proposal would allow an APP entity up to 60 days to respond before a complainant may proceed to the OAIC. Where a complaint is not resolved internally, this may unnecessarily delay access to external resolution. Consideration should therefore be given to whether 60 days is appropriate in all circumstances.

Increased powers for the OAIC

55. The Law Council is concerned that draft legislative provisions for the proposed OAIC powers and efficiency measures have not been available for consideration. While the Consultation Paper outlines the intended operation of these measures,[32] several would confer or expand significant regulatory and enforcement powers. Stakeholders should have an opportunity to scrutinise and comment on the proposed legislative provisions, including applicable safeguards, before they are introduced into Parliament.

---

30 Ibid, Chapter 4 – Controller and Processor.

31 See GDPR Art 4(1) which defines processing as "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*".

32 Consultation Paper (n 7) 38–40.

Addressing emerging technologies

56. The Law Council acknowledges legitimate community concerns about emerging technologies and their ability to raise questions about legitimate expectations of personal privacy.

57. We note that amendments proposed under the Bill would substantially change the existing privacy regime, building on measures contained in the initial tranche of reforms. In this regard, the statutory tort for serious invasions of privacy commenced on 10 June 2025 and there may be scope under this new right to address some of the privacy harms arising from emerging technologies. We suggest that Government monitor the development of jurisprudence in this area and its potential application to emerging technologies.

58. However, we have also heard concerns that the previous and proposed amendments are insufficient to address emerging technologies. It has been suggested that, while retaining the technology-neutral approach of the Privacy Act, consideration could be given to whether the existing APP code-making framework could be used or enhanced to respond to particular privacy risks arising from new and emerging technologies.

59. The Government may also wish to reconsider other relevant recommendations of the Privacy Act Review that have not yet been actioned but may address privacy concerns. For example, Proposal 13.1 would require APP entities to undertake privacy impact assessments before commencing activities with high privacy risks. Implementation of that proposal may provide a technology-neutral mechanism for identifying and addressing privacy risks associated with higher-risk uses of emerging technologies, and support a privacy-by-design approach.

Contact

60. If you have any questions or if you would like to arrange a meeting, please contact Nathan MacDonald, Deputy General Manager, Polic[redacted] n the first instance.

Yours sincerely

Elizabeth Shearer
President-Elect