

18 September 2026

Attorney-General's Department
Robert Garran Offices
Barton ACT 2600

Via online form.

Re: Privacy Reform - Consultation on Exposure Draft legislation

To Whom It May Concern:

The Association of Digital Service Providers Australia New Zealand (DSPANZ) welcomes the opportunity to provide feedback on the proposed amendments to the *Privacy Act 1988*.

DSPANZ members provide accounting, payroll, employment, superannuation, taxation and other business software used by businesses to meet their regulatory and administrative obligations.

As the peak business software association in Australia, we strongly support contemporary privacy protections that build trust in digital services. We highlight that these reforms must preserve the ability for businesses to use data and modern technology responsibly to improve security, productivity, compliance and service delivery.

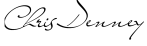
DSPANZ broadly supports clear accountability, data minimisation, stronger breach response and technology-neutral rules. These reforms will work best where responsibility follows function and control, and the requirements can be implemented consistently through software used at scale.

DSPANZ recommends that the Government:

1. ensure the controller and processor framework clearly allocates responsibility according to actual function and control, including where a processor is dealing with a non-APP entity;
2. provide OAIC guidance outlining how proportionality, lawful bases and repeatable assessments apply to business as well as AI and analytics tools or processes.
3. ensure data minimisation, retention and destruction requirements work together and recognise statutory record keeping obligations;
4. clarify that generated or derived personal information is confined to outputs actually created, retained or used about an individual;
5. coordinate controller and processor notification duties and harmonise core information requirements across Commonwealth data breach reporting; and
6. allow sufficient time after regulatory requirements are finalised for DSPs to design, build, test and support the customer transition.

DSPANZ welcomes the opportunity to provide further feedback on our submission. Please contact Maggie Leese at maggie@dspanz.org for more information.

Yours faithfully,

Signed by:

E3E80D8A0D7A7097

Chris Denney,
Interim CEO & Executive Director
DSPANZ.

About DSPANZ

Digital Service Providers Australia New Zealand is the gateway for the government into the dynamic, world-class business software sector in Australia and Aotearoa New Zealand. [Our members](#) range from large, well-established companies to new and nimble innovators working at the cutting edge of business software and app development on both sides of the Tasman.



1. Privacy obligations should follow function and control

DSPANZ supports the proposed controller and processor framework and believes this reflects modern software services. A DSP may act as a processor when processing personal information on a customer's documented instructions, while acting as a controller for a separate activity such as account administration or user verification. Responsibility should follow the relevant activity and matters each organisation controls.

DSPs may provide the same products and services to customers that are both within and exempt from the Privacy Act. In practice, DSPs are likely to apply the same contractual, technical and operational arrangements across their customers.

DSPANZ believes that the proposed framework should not depend on both parties being APP entities. If this is specifically distinguished in the Act, it will mean the same underlying software processing activities must be treated differently depending on whether the customer is an APP entity. The government should clarify how the controller and processor framework should operate in software settings and ultimately avoid unintended differences in how a DSP should provide otherwise equivalent processing activities.

We also believe that through not prescribing a format or template for documented instructions that DSPs should be able to express them in contracts, terms of use or data processing terms.

Recommendation 1:

Ensure the controller and processor framework clearly allocates responsibility according to actual function and control, including where a processor is dealing with a non-APP entity.

2. Fair and reasonable handling should enable beneficial technology

DSPANZ broadly supports a principles-based fair and reasonable test. The test should weigh potential privacy harm against the legitimate benefits that are delivered through business software including fraud detection, anomaly monitoring, cybersecurity, automation, artificial intelligence (AI), regulatory compliance and improved service delivery.

There is also a need to recognise that software applies repeatable processes at scale. An accounting practice management software platform may use the same validated workflow for thousands of their customers to onboard new clients. It should be possible to assess that design once and apply the assessment consistently.

Consent should be voluntary, informed, current, specific and unambiguous as well as required for genuinely sensitive activities. DSPANZ cautions against excessive consent that

produces friction and 'consent fatigue' in routine software processing where businesses are performing regular and routine payroll, tax, superannuation or payment activities.

Practical guidance from the Office of the Australian Information Commissioner (OAIC) should demonstrate how the test can be applied by software platforms in a consistent way. This would preserve the flexibility of a principles-based framework while allowing DSPs to translate it into repeatable product and governance decisions.

Recommendation 2:

Provide OAIC guidance outlining how proportionality, lawful bases and repeatable assessments apply to business as well as AI and analytics tools or processes.

3. Minimisation and deletion must reflect legal and technical realities

DSPANZ strongly supports data minimisation and reducing unnecessary retention.

However, DSPs commonly support customers in meeting their legislative record keeping obligations, such as employment, payroll and taxation records. Privacy requirements should not require the destruction of information that must legitimately be retained for another statutory purpose. This principle is particularly important if the right to erasure is more broadly applied to APP entities in the future. For example, deleting an employee's payroll record on request could prevent an employer meeting their record keeping and reporting responsibilities.

The proposed requirement to identify the personal information an organisation holds should remain technology neutral. It should not encourage organisations to duplicate or centralise personal information simply to demonstrate that they know where it is held, as doing so could increase security exposure.

The requirement to reassess de-identified information should be proportional to material changes in risk and not unintentionally require continuous reassessment due to analytical capability advances.

Recommendation 3:

Ensure data minimisation, identification, retention, destruction and de-identification requirements work together to reduce the unnecessary holding of personal information while recognising statutory retention requirements and proportionate technical measures.

4. The scope of personal information should remain practical

DSPANZ supports recognising that personal information may be generated or derived through data analysis, AI and other technologies, but not at every possible inference. System logs, metadata and temporary calculations may help validate a transaction without becoming information used about an individual.

For example, a risk score discarded after a payment check should be distinguished from a stored score used to make later decisions. A temporary result that is not subsequently used as information about the individual should be distinguished from an inference that a system actually makes and uses.

Recommendation 4:

Clarify that generated or derived personal information is confined to outputs actually created, retained or used about an individual.

5. Data breach reform should reduce regulatory fragmentation

DSPANZ supports earlier breach response, harm mitigation and the proposed 72-hour notification period, including the ability to supplement an initial notification as more information becomes available.

The alignment of reporting timeframes is useful, but DSPs responding to a significant cyber incident may still need to report substantially the same incident under multiple Commonwealth regimes using different requirements.

For example, a DSP may need to provide information about the nature of an incident, affected systems and remediation activities to several government bodies. Requiring that information to be repeatedly reformatted to suit each reporting framework does not improve incident response and can divert resources from containment and recovery.

We also recognise that a cloud incident may involve multiple parties, including the customer, DSP, hosting provider and identity service provider. Guidance should clearly identify who is responsible for the data breach notification and escalating the incident, so affected individuals do not receive inconsistent messages.

DSPANZ supports greater alignment across Australia's cyber reporting frameworks. Common information should be defined consistently and be reusable across reporting obligations wherever practicable.

Recommendation 5:

Coordinate controller and processor notification duties and harmonise core information requirements across Commonwealth data breach reporting.

6. Implementation

The proposed reforms may require changes to product architecture, contracts, integrations, notices, consent flows, data inventories and incident procedures.

DSPs need sufficient certainty about the final legislation and regulatory expectations before they can design, build and test those changes. Supporting material should explain how clear legislative requirements operate rather than resolve fundamental questions about their scope.

The transition period should begin once legislation and supporting material are settled. The OAIC should consistently engage with DSPs so that they can translate the reforms into systems used by businesses at scale.

Recommendation 6:

Allow sufficient time after regulatory requirements are finalised for DSPs to design, build, test and support the customer transition.