dspanz. digital service providers australia new zealand

217 Flinders Street
Adelaide SA 5000
hello@dspanz.org
dspanz.org

31 March 2023

Attorney-General's Department
Robert Garran Offices
3-5 National Circuit
Barton ACT 2600

Via online form.

Re: Privacy Act Review Report Submission

To Whom it May Concern:

The Association of Digital Service Providers Australia New Zealand (DSPANZ) welcomes the opportunity to make this submission on behalf of our members and the business software industry.

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 90+ members range from large, well-established companies through to new and nimble innovators who are working at the cutting edge of business software and app development on both sides of the Tasman.

DSPANZ welcomes the Privacy Act Review Report (the Report) and many recommendations which will enhance privacy protections across Australia. In particular, we support the proposals that better align the Privacy Act (the Act) with the European Union's General Data Protection Regulation (GDPR) and other international privacy standards.

Digital Service Providers (DSPs) create, sell and use software solutions to assist with the day to day management of a business, its critical suppliers, business processes and employees. DSPs capture, use, retain and disclose data relating to both businesses and individuals to facilitate business processes and assist with their record-keeping and reporting obligations. DSPANZ anticipates that changes resulting from the review will create varying impacts for DSPs and how they provide software and services to their end users.

In summary, this submission raises the following:

- Overall comments on how the Act aligns with GDPR, the importance of consultation with DSPs and the importance of being able to leverage digital identity and business registry services;

- It is crucial to consider the flow-on effects of updating the definition of personal information as it may impact other security incident or data breach reporting obligations across Australia;
- We are interested in working through any potential implications or unintended consequences regarding employment-related reasons for collecting, using and storing geolocation data;
- If the small business exemption is removed, it is essential to also consider the role DSPs will play in making changes and educating their small business users;
- We believe the employee record exemption should largely remain in place but with changes to protect employees and their data better;
- DSPs are required to follow record-keeping requirements under existing employment and taxation law which may create challenges around data retention requirements and the right for individuals to access or erase their personal data;
- Whether automated rostering processes would be classified as automated decision making if the employee record exemption is modified or removed;
- Any penalties within the Act should be aligned proportionally to the size and revenue of an organisation.

DSPANZ welcomes the opportunity to provide further feedback on our submission. Please contact Maggie Leese for more information.

Yours faithfully,

Matthew Prouse,
President & Director
DSPANZ.

Overall Comments

Alignment with GDPR

As mentioned, DSPANZ supports proposals that better align the Act with GDPR as it will support Digital Service Providers (DSPs) who operate internationally and are required to meet the regulation. However, if the Act deviates from GDPR, it will place a significant regulatory burden on global organisations that must manage competing requirements.

Consultation with DSPs

We recognise that a revised Act will involve a level of change for organisations across Australia. It will therefore be necessary for the government to consult widely on the appropriate timeframes required to meet any changes resulting from the review.

For DSPs, there can be two levels of change involved when meeting new or revised legislation:

1. Changes DSPs are required to meet as an organisation; and
2. DSPs must implement changes in their software to assist end users in meeting their obligations.

DSPs will face different challenges when implementing changes depending on their size, resourcing and system architecture.

This is why we consider formal consultation with DSPs on any changes affecting tax, accounting, payroll, business registry or superannuation obligations critical. This consultation would help establish appropriate timeframes for implementation and, further, the time required for any end-user education.

Digital identity and business registry services

There are two key pieces of technology that will play an important role in supporting organisations in meeting a revised Privacy Act:

1. Low or no-cost public digital identity solutions that DSPs can leverage to verify both individuals and businesses; and
2. A contemporary set of business registers that will provide higher integrity data for DSPs and natural business processes to rely on.

With these solutions in place, we anticipate it will be much easier for organisations, in particular DSPs, to meet their obligations under the Act.

Personal information, de-identification and sensitive information

Definition of personal information

The proposed clarification to the definition of personal information may create challenges for DSPs when determining whether or not a breach of personal information has occurred within their systems. While there are impacts for those who are required to report under the Notifiable Data Scheme (NBD), DSPs are also required to report breaches of personally identifiable information under the Australian Taxation Office's (ATO) Operational Security Framework. A broader definition may make it difficult for DSPs to determine whether personal information has been affected in an incident.

It is crucial to consider the flow-on effects of updating the definition of personal information as it may impact other security incident or data breach reporting obligations across Australia.

The recognition of IP addresses and device identifiers as personal information, where it relates to a reasonably identifiable individual, may create additional challenges for DSPs who are required to record this information as a part of audit logging requirements under the ATO Operational Security Framework and other security standards such as the Security Standard for Add-on Marketplaces (SSAM). This requirement would particularly impact the many DSPs running cloud-based systems and workforce management software who collect this data for geolocation purposes. DSPs who collect this data must encrypt their audit logs if IP addresses and device identifiers are classified as personal information.

Geolocation data

DSPANZ is interested in working through any potential implications or unintended consequences regarding employment-related reasons for collecting, using and storing geolocation data. We would like to balance providing adequate privacy protections and seamless experiences for software users.

With potential changes to the employee records exemption, a number of our members providing payroll and workforce management software who collect, use and store geolocation data are interested in clarifying whether there will be any implications around collecting this data for employment-related purposes. We note some fundamental payroll and invoicing processes rely on this data to make accurate payments.

Examples of where DSPs may use geolocation data include:

- Ensuring employees are at their place of work when they are clocking in and out.
- Checking in and out of multiple work sites.
- Job or progress tracking.
- Moving between clients during the day.
- Calculating the distances between jobs.

While this data is typically used for payroll and invoicing purposes, it may also be used to provide valuable insights and analysis to employers such as allowing them to make better rostering or job allocation decisions.

We acknowledge that access to any geolocation data within systems should be restricted to the individual and the primary user to which an individual gives this consent. Further, this data should not be shared with any third parties other than for purposes related to their employment outside of the defined use cases that an individual consents to.

Small businesses

Removing the small business exemption
If the small business exemption is removed, not only will there be a considerably significant impact on small businesses, but there will also be flow-on implications for DSPs who provide software for small businesses, many of whom are small businesses themselves. This would include implementing any changes in software while also supporting and educating their small business users.

Similarly, almost all IT providers and implementors would be heavily impacted if the exemption is removed.

We highly recommend consulting extensively with small businesses, DSPs and others that support small businesses to understand better the significant amount of time they will need to operationalise the removal of the exemption.

Impact of penalties on small businesses
While we support the proposals to introduce a tiered penalty approach, we strongly recommend that penalties applying to small businesses should be aligned to their size.

Any data breach is likely to be a business extinction event, regardless of penalty size, for a small business. It is doubtful that many Australian small businesses will have sufficient funds or resources to recover from the financial, brand and reputational damage caused by a data breach. Consequently, increasing penalties into the tens of millions of dollars will only create further economic costs for small business owners as they exit their businesses.

Employee records

Removing the employee records exemption
DSPANZ believes that the employee record exemption should largely remain in place but with changes that will better protect employees and their data. For our members, this exemption is critical to allow employers to perform tasks across payroll; human resources and; occupation, health and safety. DSPs can also offer innovative ways to enhance company efficiencies and improve corporate practices with this data.

An example of where protections could be enhanced includes removing the ability for an employer to provide employee information to third parties where the disclosure is not for a purpose related to the employment relationship, and the majority of employees would not provide active consent. This could include giving a credit agency “all” employee payroll records if one of their employees chooses to apply for a loan with a related lender.

We would also like to acknowledge the role that software plays in keeping employee data secure, given the security requirements DSPs must adhere to under the ATO's DSP Operational Security Framework or the Security Standard for Add-on Marketplaces (for the line of business applications not directly connected to the ATO or storing payroll, tax or superannuation data).

DSPANZ asks to be involved in any consultation on enhanced employee protections. We are particularly interested in avoiding any unintended consequences to the interactions and processes that DSPs facilitate on behalf of employers and employees or the requirements to meet multiple government department standards for data security.

Giving an appropriate timeframe for DSPs to implement any changes
If any changes are made to the data collection requirements around employee records, including changing or removing fields, it will require changes within software.

It is important for the government to understand that many DSPs have built systems around the employer exemption and employer requirements for record-keeping over employee rights to delete. Retrospectively updating systems that have been developed over many years would be at a considerable cost and may result in some DSPs exiting the market. If there are DSPs who leave the market, it could result in a significant negative impact on businesses as their systems no longer work, and they may lose access to data as DSPs move to cover themselves and their obligations under the Act.

We ask the government to specifically consult with DSPs on the timelines required to make such changes and educate users.

Rights of the individual

Introducing the right for individuals to access, object, erase, correct or de-index their personal information will create conflicts with existing record-keeping requirements.

We anticipate that many DSPs will be unable to offer these individual rights as intended as DSPs must follow record-keeping requirements outlined in existing legislation, including the Fair Work Act, state-based long service leave legislation and taxation law (noting that the Taxation Administration Act supersedes the Privacy Act).

Further, as many DSPs operate business to business, they have a relationship with those who purchase the software or services and not the employees themselves. This makes it more complicated for DSPs to implement individual actions and processes that apply to employees.

Automated decision making

Our members have raised concerns about whether automated rostering processes may be classified as automated decision making if the employee record exemption is modified or removed. We are interested in understanding whether there will be any impacts to this type

of automation, and if so, we ask the government to consult with rostering, time and attendance software providers.

Security, retention and destruction

Security
The current proliferation of security standards and controls makes it difficult for many organisations, especially small businesses, to navigate and determine the best approach. In guiding baseline privacy outcomes, we recommend avoiding the creation of a new set of security requirements that organisations must adhere to.

We note that many DSPs currently meet the ATO's DSP Operational Security Framework or the Security Standard for Add-on Marketplaces and, as a result, will meet recognised security standards, including ISO 27001 and similar government-specific standards such as the Information Security Manual (ISM) and the National Institute of Standards and Technology (NIST).

Retention periods
DSPs will have different approaches to their minimum and maximum data retention periods due to the additional legislation they must comply with. While maximum periods are typically 5 to 7 years, as required by employment and taxation law, other pieces of data may need to be kept for more extended periods. For example:

- Employers needing to calculate long service leave entitlements must access employee data for their organisational tenure.
- Employers may need to keep records of worker's compensation claims indefinitely, even after an employee leaves the organisation.
- Employers needing to maintain records of disciplinary action.

Many DSPs are thinking through their data retention practices in light of recent high-profile cyber-attacks. While DSPs must comply with record-keeping requirements, they also balance their customer's expectations around how long their data should be kept for, especially once they are no longer paying customers. As a community, we are currently looking at data minimisation and retention practices to help set expectations for both DSPs and their customers.

If the employment exemption is removed, data retention requirements must be reviewed and addressed across all legislation to ensure alignment with the Act. Further, employers should not be penalised for not holding data that an employee has requested to be removed.

DSPANZ would be interested in participating in any consultation around the review of data retention requirements and any new proposals.

Controllers and processors of personal information

While we support the alignment that would be created between the Act and GDPR with the introduction of controllers and processors, it would not necessarily benefit DSPs in terms of reducing any obligations around data retention and data breach reporting. We recommend

the creation of a third role designed to help individuals who need to be more experienced with the legislation and who have delegated authority to act on behalf of an individual.

Overseas data flows

DSPANZ supports recommendation 23.6 of the report as this will provide suitable coverage for DSPs who may disclose personal information to overseas recipients.

Notifiable data breach reporting scheme

DSPANZ is interested in participating in any consultation around assisting organisations with multiple data breach reporting obligations and aligning security requirements with other schemes.

Enforcement and statutory tort for serious invasions of privacy

DSPANZ believes that any penalties should be proportional to the organisation's revenue to ensure that they take the impact of their failure to comply seriously.