Queensland Law Society

Law Society House, 179 Ann Street, Brisbane Qld 4000, Australia
GPO Box 1785, Brisbane Qld 4001 | ABN 33 423 389 441
P 07 3842 5943 | F 07 3221 9329 | president@qls.com.au | qls.com.au

Office of the President

22 March 2023

Our ref: [PDTIP:KS]

Confidential

Dr James Popple
Chief Executive Officer
Law Council of Australia
GPO Box 1989
CANBERRA ACT 2601

By email: [redacted]

Dear Dr Popple

Government response to the Privacy Act Review Report

Thank you for the opportunity to provide feedback to inform the Law Council's submission to the Attorney-General's Department in relation to its Privacy Act Review report (**the Report**).

This response has been compiled with the assistance of the QLS Privacy, Data, Technology and Intellectual Property Law Committee.

Introductory comments

QLS has for a number of years advocated for reform of state and federal privacy laws including the creation of a statutory framework which provides greater protection of the privacy of individuals and the harmonisation of federal, state and territory privacy laws. We welcome the Report and progressed reform in this area.

We highlight that given the high level nature of the various proposals, it may be that there are further issues which are identified during the legislative process which we have not identified. We submit that the proposed reforms should be viewed within the context of the Australian privacy framework as a whole. Early and reasonable consultation with key stakeholders on any draft legislation will be critical.

The QLS response to this stage of the government's response to the Report is limited to those areas outlined below.

Small business exemption

QLS has previously submitted that the current small business exemption does not strike the right balance between protecting the privacy rights of individuals and the avoidance of compliance costs. The proposal to remove the small business exemption recognises the public interest in protecting privacy. Consistent with the proposed amendment to the objects of the *Privacy Act 1998* (Cth) (**the Act**), this is a fundamental principle and should underlie reforms in this area. However, our members have also recognised that there are a range of considerations at play in ensuring that reasonable and proportionate obligations are imposed on small businesses.

QLS supports the Report's proposed approach which reflects the need for impact analysis, stakeholder consultation and comprehensive assistance being made available to small businesses prior to removing the exemption. In the shorter term, the proposals outlined in 6.2 with respect to prescribing the collection of biometric information for use in facial recognition technology as an exception to the small business exemption and removing the exemption for small businesses who trade in personal information appears to be appropriate. The drafting will be important, particularly in relation to what amounts to 'trading in personal information'. For example the Report proposes that 'trading' in personal information would be broader than the sale of information and include for example reciprocal data sharing/matching, even where not for a fee.[1]

Implementation issues

Our members have also identified some areas in which the Report has not fully contemplated the scope of potential issues and nuances in implementation.

Firstly, legislative reform to the privacy framework must be supported by appropriate regulatory guidance. The Office of the Australian Information Commissioner (**OAIC**) should be resourced to support businesses in understanding their obligations and in complying with the Act. This should include resources to support entities coming under the expanded scope of the Act and guidance around the intended scope of 'trading in personal information'.

The Report recognises that the OAIC would need to be resourced to provide support to meet the needs and any challenges experienced by small businesses to adopt the privacy standards in the Act. This will be a significant undertaking and it is not yet clear what resources will be sufficient and/or of most assistance.

The private sector, including the legal profession, will play an important role in supporting businesses (particularly small business clients) through any reforms. As noted earlier, consultation with stakeholders, including with the profession early on will be essential.

[1] *Privacy Act Review* (Report, 2022) p 210.

Secondly, whilst the Report considers in detail the situation of a small business as a data processer, a further challenge for small business will be how to manage Notifiable Data Breaches (**NDB**) and related obligations as *controllers*, especially where the breach has occurred at the processor level.

It is rightly recognised in the Report that the use of third party online platforms / Software as a service (**SaaS**) by small business has increased both the risk and consequences of data breaches. This software encourages (or even demands) the collection of large amounts of personal information from customers that in many cases is not strictly necessary. It is however, rarely feasible for small business to tailor these systems to capture less information, even if they wanted to do so. Under the proposed reforms, small business may therefore be left with a situation where software vendors will be permitted to pass much of the risk arising from over collection / breach to small business users, as those vendors will only be processors.

Thirdly, some of our members have queried the extent to which the prospect of Australia obtaining an EU adequacy decision justifies, or necessitates, the removal of the small business exemption *in its entirety*. It is understood that an adequacy ruling would not exempt Australian businesses from complying with the GDPR, if otherwise falling directly within the GDPR's jurisdiction. Further, only 12 countries or territories have ever been recognised under the adequacy scheme.[2] There is also scope for the EU to *review* decisions made under the pre-GDPR scheme. Therefore, consistent with proposal 6.1 of the Report, an impact analysis could encompass a costs / benefits analysis of seeking an adequacy ruling, and if so on what terms, perhaps undertaken by the Productivity Commission.

In comparison, the United States' data privacy framework, which is currently under consideration by the EU and widely expected to pass in some form, will be more limited in scope and will not require such an extension to all businesses.[3] The Report also notes that the UK Government has recently proposed more flexibility for business than the GDPR allows.[4]

Whilst strengthened privacy frameworks in Australia are crucial, research suggests that small firms in the UK have experienced the main burden of the GDPR.[5] Although this may reflect a temporary adjustment,[6] this context nevertheless reiterates the need for considered reforms, transitional arrangements as well as early partnerships with regulators to ensure that issues

---

[2] Excluding the UK, whose compliance is related to its status as a former EU member, only Japan and South Korea have been granted this status since the GDPR was introduced in 2016 (both significant data processors). See: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[3] The US Data Privacy Framework (DPF) is working its way through the EU process at present, but it would not apply to all businesses in the United States. (See European Data Protection Board, Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework (Adopted on 28 February 2023), para 8 https://edpb.europa.eu/system/files/2023-02/edpb_opinion52023_eu-us_dpf_en.pdf.

[4] Page 58.

[5] Chinchih Chen et al, 'Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally' (2022) *Oxford Martin School, University of Oxford* p 2.

[6] See for example Chinchih Chen et al, 'Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally' (2022) *Oxford Martin School, University of Oxford* p 25.

impacting businesses are addressed as they emerge and careful consideration is given to what is reasonable in terms of compliance and the privacy rights of individuals.

Legal profession specific issues

As the Law Council would be aware, it is also important to highlight that an estimated 82% of law practices in Australia are sole practitioners[7] and an even greater number would be small businesses within the existing small business definition ($3 million turnover). Therefore, apart from those who may already be covered by an exception to the current exemption (for example, personal injuries law practices holding medical information), privacy compliance will be a significant issue and will add to overhead costs. This is likely to be reflected in access to justice issues including higher fees, particularly in regional and remote areas.

Further, some of the proposed reforms may be problematic for smaller firms to manage without appropriate exemptions. For example, to comply with the proposed right of erasure there will need to be processes in place to allow client files to be held without redaction. It may also be complex for these firms to establish whether personal information on a client file belongs to / ought to be the responsibility of the firm for the purposes of the Act.

Practical measures to support implementation

In addition to the implementation issues identified to be considered above, our members have suggested further practical measures to strengthen the proposals in the Report as set out below.

1. We support the proposed use of measures including template privacy policies (which can be modified based on different risk factors) and the New Zealand Privacy Commissioner's privacy statement generator.

   A default or basic privacy policy could also be included in the legislation, perhaps like replaceable rules, to help overcome the risk that compliance material not suited to this jurisdiction, or substandard material, will be used by many businesses for cost reasons.

2. Australian Privacy Principles (**APPs**)

   Lastly, it has been suggested that the complexity of the existing scheme derives from the fact that the APPs were designed mostly for larger businesses. A shorter, plain English document, code or charter for small business, instead of or to supplement the APPs may better support smoother implementation.

Direct marketing, targeting and trading

The way in which personal information is handled for marketing purposes, and the privacy risks associated with direct marketing, have changed dramatically since the APPs were first introduced in 2014. The proposed reforms in the Report are in response to the significant

[7] National Legal Profile (2021): https://www.lawsociety.com.au/sites/default/files/2021-07/2020%20National%20Profile%20of%20Solicitors%20-%20Final%20-%201%20July%202021.pdf.

community concern with respect to direct marketing activities, particularly with respect to children. The proposals in the Report seek to address the change in practices and increased risk of privacy harm as a result.

Prohibiting targeting to a child

QLS strongly supports the proposed changes with respect to children's online privacy although clear guidance will be needed as to the interpretation of what is 'in the best interests of the child' to assist organisations and legal advisors as to what this means in practice.

Our members have noted there is good guidance domestically via the eSafety Commissioner and from other jurisdictions as to age appropriate design and marketing. For example, as outlined in the Report, the best interests test has been adopted in the UK Age Appropriate Design Code and the Irish Data Protection Commission's Fundamentals for a Child-Oriented Approach to Data Processing.[8]

Unqualified right to opt-out of use or disclosure of personal information for direct marketing

Proposal 20.2 seeks to provide individuals with an unqualified right to opt-out of their personal information being used or disclosed for direct marketing purposes.

Our members highlight that one of the complexities in operationalising compliance with the existing APP 7 is the exclusion of APP 7 to the extent the *Spam Act* and *Do Not Call Register Act* applies. This can be complex for organisations looking to manage consent and communication preferences in a centralised database across multiple channels, although there are technology tools that can assist with this.

In this regard, the Report does not, unfortunately, contain proposals to help harmonise the requirements, but it does suggest further consultation. In our view, it would be beneficial to consider some harmonisation in this area in conjunction with progressing the current reform proposals.

Legal profession specific issues

For the legal profession, the main impact would likely be with respect to the tightening of the consent and opt-out requirements, restrictions on targeted online advertising, and the increased level of transparency as to any targeted practices. It is assumed that law practices are otherwise already complying with their obligations under APP 7 and not (generally) trading in personal information or targeting children.

However, existing state and territory advertising restrictions, including for example Queensland's claims farming and personal injury advertising restrictions should also be considered in the context of regulating directing marketing practices here.

[8] Page 152. See also in the United States the federal *Children's Online Privacy Protection Act* (COPPA) and the California Age-Appropriate Design Code (CA AADC).

Overseas data flows

Finally, proposal 23.1 of the Report recommends consultation on an additional requirement in subsection 5B(3) of the Act to demonstrate an 'Australian link' that is focused on personal information being connected with Australia.

The *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022* (Cth) recently sought to remove the requirement that a foreign organisation must collect or hold personal information directly from a source in Australia in order to have an 'Australian link'. This means that foreign organisations doing business in Australia would be more likely to be subject to the Act, including the APPs and the NDB scheme.

We support recommendation 23.1 for further consultation. This concerns the appropriate extent of the Act's "long arm". If other countries enacted a similar extra-territorial reach to subsection 5B (as now amended), it would mean Australian businesses which also carry on business in those other countries would be bound by the countries' domestic privacy law, regardless of any connection at all with their residents' personal information. We agree that a further amendment addressing the missing concept of the personal information being connected with Australia warrants the recommended consultation.

Recommendation 23.2 concerns introduction of a mechanism to prescribe countries and certification schemes which give substantially similar protection to the APPs. We support this recommendation. It would provide much needed clarity for Australians (individuals and businesses of all sizes) regarding the adequacy of ex-Australian privacy laws to which Australian-sourced personal information will be subject.

Recommendation 23.3 is for there to be template standard contractual clauses available to APP entities for use when transferring personal information overseas. We would regard this as a significant privacy-positive step for compliance purposes but support the suggestion that the standard clauses be drafted in a way which is aligned, as far as possible and meaningful, with the standard clauses which have been promulgated elsewhere.

If you have any queries regarding the contents of this letter, please do not hesitate to contact our Legal Policy team via [redacted]

Yours faithfully

[redacted]

Chloé Kopilović
President