Australian Government | TAX PRACTITIONERS BOARD

15 May 2026
Our ref: 06.26OM

Committee Secretary
Joint Committee of Public Accounts and Audit
PO Box 6021
Parliament House
Canberra ACT 2600

Sent by email to: jcpaa@aph.gov.au

Dear Committee Secretary

Inquiry into the management of client privacy in the Australian public sector

The Tax Practitioners Board (**TPB**) welcomes the opportunity to make a submission to the Joint Committee of Public Accounts and Audit (**Committee**) in relation to the inquiry into the management of client privacy in the Australian public sector (**Inquiry**).

Background

The TPB is an independent statutory body that administers the *Tax Agent Services Act 2009* (**TASA**). The TPB is responsible for registering and regulating tax agents and BAS agents (collectively referred to as 'tax practitioners'). Over 60,000 tax practitioners are registered with the TPB.

The object of the TASA is to support public trust and confidence in the integrity of tax profession and of the tax system by ensuring that tax agent services are provided to the community in accordance with appropriate standards of professional and ethical conduct.

TPB comments

The Inquiry's terms of reference focuses on public service entities' identification and management of privacy risks, their response strategy to information security breaches and threats, and matters related to the Australian National Audit Office Auditor-General's report '*Managing the Privacy of Client Information in Services Australia*' (**Report**). This submission provides general comments relating to how the TPB manages client privacy in relation to Recommendations 4 and 5 of the Report. Importantly, the TPB's 'client' data relates to a specific registered tax practitioners population set and generally does not include broader information relating to the general public.

As an Australian Government agency, the TPB is required to comply with the Australian Privacy Principles (**APPs**) under the *Privacy Act 1988* (**Privacy Act**) when collecting and holding personal information for the purpose of exercising our powers and administering our functions under the TASA.

At a broad level, the TPB collects personal information only when it is necessary to carry out its responsibilities under the TASA which are generally as follows:

- administer a system to register tax practitioners including processing and investigating applications for registration
- investigate conduct that may breach the TASA and imposing sanctions for breaches

- administer a system to accredit professional associations as recognised tax agent or BAS agent associations
- maintain a publicly available register of registered and deregistered tax practitioners as required by the TASA
- respond to requests for access under the *Freedom of Information Act 1982* (**FOI Act**) and requests for official information from the ATO, ASIC and authorised law enforcement agencies
- provide guidelines, policy and information on matters relevant to the administration of the TASA
- publish communications on matters relevant to the administration of the TASA, including media releases, speeches, event details, newsletters, surveys and social media posts.

The TPB is subject to secrecy provisions which prohibits the disclosure of official information to a third party, unless a relevant exception applies.[1] The TPB is also subject to restrictions on the use and disclosure of information under the Privacy Act and APPs. Some examples of when the TPB may collect personal information from a third party includes:

- when a complaint or breach report relating to a tax practitioner is received
- in the course of undertaking risk assessments, preliminary enquiries and investigations into conduct that may breach the TASA
- in the course of legal proceedings.

The TPB's Legal Unit oversees the management of the personal information it collects, including matters relating to freedom of information (**FOI**), privacy and TASA disclosures. This work is undertaken in line with the Office of the Australian Information Commissioner's (**OAIC**) procedures and guidance for managing FOI requests.

The TPB has a robust process in place to protect personal information held by the TPB from loss, unauthorised access, use, modification, disclosure and misuse. This includes:

- daily backups to prevent data loss
- restricting access to the TPB's information technology (IT) system through a number of controls, including password-controlled entry, multifactor authentication and single sign-on.
- granting TPB system access only to approved users
- regular auditing, monitoring and reviewing access to the TPB's IT system ensure access is limited to those that require it
- maintaining internal quality assurance processes to protect personal information, including verification of the accuracy of personal information prior to use.

The TPB manages privacy risks in accordance with the Protective Security Policy Framework (PSPF). This includes strict authentication controls (such as multifactor authentication) for access to sensitive information, regular reviews of user access, timely offboarding of departing staff, and active prevention, risk assessment and monitoring of potential information leaving the organisation.

It is important to acknowledge the significant overlap between information regulated under privacy laws and information regulated under secrecy provisions. As a result, the TPB's approach to managing privacy and secrecy information is closely aligned.

The management of information is primarily centred on controlling the 'gateway' through which information is received and disseminated. This is supported by the technological infrastructure underpinning the TPB's information management processes. Key elements include:

[1] Section 70-35 of the TASA.

- proof of identity and verification requirements
- defined processes for the sharing and disclosure of information with other government agencies, undertaken in accordance with both privacy and secrecy law requirements,
- completion of Privacy Impact Assessments (PIAs) where a Privacy Threshold Assessment identifies a privacy risk for any new data programs or material changes to existing programs. The TPB publishes details of the PIAs that are undertaken on a register on the TPB's website.

In the event of a data breach, the TPB has a mature, reviewed and audited Incident Response Procedure that guide actions and priorities during a cyber incident. The TPB conducts a breach assessment when there has been a data breach in accordance with OAIC guidelines and responds to data breaches in compliance with the Privacy Act and OAIC guidelines. The TPB's approach consists of three main steps:

1. Prevention
    - Maintain appropriate and reasonable processes to protect personal information.
    - Implement systems and IT controls to safeguard electronically held data.
    - Provide staff training on the handling and disclosure of personal information.
    - Reduce the likelihood of a data breach occurring.
2. Limitation
    - Minimise the consequences or likelihood of harm to affected individuals.
    - Remove any accidentally published information from the register as quickly as possible.
    - Notify affected individuals so they can take steps to mitigate the breach (where required).
    - Apply immediate technological or process changes to stop the breach and prevent recurrence.
3. Rebuild
    - Maintain confidence among tax practitioners and the broader public in the TPB's management of personal information.
    - For significant incidents, engage the TPB Communications team to support media response and strategy.
    - Involve the TPB Client Services team to manage external enquiries related to the breach.

We welcome any additional discussions or assistance we can provide to the consultation. If you have any queries in relation to the TPB's submission, please contact

Yours sincerely

Andrew Orme
Secretary
Tax Practitioners Board