Australian Government
Australian Taxation Office

ATO Submission

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

15 May 2026

Contents

Introduction

1. The Australian Taxation Office (ATO) welcomes the opportunity to provide a submission to the Joint Committee of Public Accounts and Audit (JCPAA) *Inquiry into the management of client privacy in the Australian public sector*.
2. The ATO handles the personal information of millions of Australians every day in connection with the administration of Australia's federal tax, superannuation and related systems.
3. The ATO treats its obligations to handle this information lawfully, ethically and securely with the utmost seriousness and care. As an APP entity under the *Privacy Act 1988* (Privacy Act),[1] the ATO is required to comply with the Privacy Act and the *Privacy (Australian Government Agencies — Governance) APP Code 2017* (APP Code).
4. In addition to the Privacy Act, Australia's tax confidentiality framework[2], imposes strict obligations on the ATO, in respect of recording and sharing the personal tax information of entities, including individuals. The framework prohibits the disclosure of tax information protected by the confidentiality provisions, except in certain specified circumstances and only where Parliament has determined that the public benefit derived from the disclosure outweighs the potential impacts on privacy and voluntary tax law compliance.
5. These provisions maintain the privacy, integrity and confidence of all entities interacting with the tax system and support high levels of voluntary compliance. Contravention of the provisions is a criminal offence.
6. The majority of personal information the ATO collects, holds, uses and discloses is necessary for, or related to, the administration of taxation and superannuation laws and other programs of work we administer[3]. As such, this information is subject to the protections of both the tax confidentiality framework and the Privacy Act. Taxation and superannuation law provide the necessary authorisation required under the APPs in respect of dealing with personal information.
7. This submission outlines the ATO's governance frameworks to identify and manage risks under both the tax confidentiality framework and the Privacy Act.

Compliance with Privacy Act and APP Code

8. The ATO has a developed and mature governance framework, which satisfies the requirements under the Privacy Act and APP Code. Under the APP Code, the ATO is required to: [4]
    a. develop a Privacy Management Plan (PMP) and assess its performance against the PMP at least annually;
    b. appoint a Privacy Champion and Privacy Officer/s; and

[1] *Privacy Act 1988* (Cth) s 6(1).

[2] Ss 8WA-8WC and Division 355 of Schedule 1 to the *Taxation Administration Act 1953* (Cth) (TAA).

[3] The ATO also handles personal information in its role as a Commonwealth agency and employer. For example, personal information of staff/contractors.

[4] https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/government-agencies/australian-government-agencies-privacy-code/privacy-australian-government-agencies-governance-app-code-2017

c. conduct Privacy Impact Assessments (PIAs) for all high privacy risk projects and initiatives and maintain a PIA register.

Privacy Management Plan

9. The ATO develops an annual PMP which measures and monitors compliance with its privacy obligations and conducts an annual performance assessment of its PMP against the Office of the Australian Information Commissioner's (OAIC's) Privacy Maturity Assessment Framework.[5]
10. The annual PMP and performance assessment are approved by the Privacy Champion (see paragraph 14).
11. For the 2023-24, 2024-25 and 2025-26 financial years (FY), the ATO has self-assessed its privacy maturity as either 'Leader[6]' or 'Defined'[7] against the 21 attributes provided by the OAIC.
12. The 2025-26 FY performance assessment will incorporate the findings of internal and external review processes, such as the findings of a recent Internal Audit of the ATO's Data breach response and the data exchange review underway between the ATO and Services Australia under Recommendation 16.2 of the *Royal Commission into the Robodebt Scheme*.[8]

Privacy Champion and Privacy Officer

13. The ATO has a designated Privacy Champion and Privacy Officer,[9] who are supported by lawyers within the ATO's Office of the General Counsel (OGC).
14. The Privacy Champion is the ATO's Chief General Counsel and a Deputy Commissioner of Taxation, and is responsible for promoting a culture that values privacy and embedding privacy by design principles. The Privacy Champion provides an annual privacy brief to the ATO Executive, which includes a summary of the outcome of the annual PMP performance assessment and the number of notifiable data breaches.
15. The Privacy Officer is a Deputy General Counsel (Executive Level 2) and is supported by lawyers in OGC, who provide specialist legal advice on privacy issues, including PIAs and privacy impact threshold assessments (PITAs).
16. Whilst not required by the APP Code, the ATO maintains a Privacy Network, which consists of the Privacy Officer and representatives from each business area across the ATO. The network is responsible for assisting ATO staff in relation to privacy queries and compliance.

[5] https://www.oaic.gov.au/__data/assets/pdf_file/0005/1301/interactive-pmp-explained.pdf

[6] Means an agency's practices, procedures and systems are continuously improved and the agency help others to innovate and achieve. The ATO has assessed its maturity as 'Leader' in 8 attributes.

[7] Means that an agency's privacy practices, procedures and systems are consistent, proactive, documented, integrated into broader organisational frameworks and measured. The ATO has assessed its maturity level as 'Defined' for 13 attributes .

[8] https://robodebt.royalcommission.gov.au/system/files/2023-09/rrc-accessible-full-report.PDF

[9] https://www.ato.gov.au/about-ato/commitments-and-reporting/information-and-privacy/your-privacy/privacy-policy

17. In addition, there are specialised teams within the ATO that provide advice on data matching processes, where personal information is involved.

Privacy Impact and Ethics Assessment

18. PIAs are mandatory for high privacy risk projects and initiatives and are embedded within the ATO's corporate project and policy frameworks. For data activities using personal information (including activities using Artificial Intelligence), the ATO's enterprise data sharing framework and internal privacy, data management and AI instructions and guidance reflect the paramount importance of privacy impacts being assessed.
19. The ATO has developed guidance material and templates for PIAs and PITAs for staff and ensures compliance with the data matching protocols under OAIC's guidelines on data matching in Australian Government administration through regular review processes.
20. ATO staff must follow the ATO's Data Ethics Principles, which includes completion of a Data and Analytics Ethics Assessment for all new or significantly changed projects/data activities to ensure data is used not only lawfully, but also ethically. PIAs and Data and Analytics assessments are kept on an internal register available to all ATO staff.

Policies to manage the privacy of client information

21. The ATO maintains a suite of internal policies addressing privacy, confidentiality, data management, identity management, information security and data matching.
22. These policies take the form of corporate instructions issued by the Accountable Authority[10] and Agency Head[11], both being the Commissioner of Taxation, and compliance is mandatory for all ATO staff.
23. The failure of ATO staff to comply with Corporate Instructions may not only constitute a breach of the Australian Public Service (APS) Code of Conduct [12] but may also constitute a criminal offence, where there has been unauthorised access or unlawful disclosure of taxpayer information. The ATO treats these matters with the utmost seriousness and refers matters to the Commonwealth Director of Public Prosecutions for consideration for prosecution.
24. The ATO's various memoranda of understanding with other Commonwealth and State/Territory bodies and the ATO's data management policies stipulate detailed governance requirements for data exchanges that involve personal information, including requirements to:
    i. obtain legal guidance from OGC on the lawfulness of the exchange based on the complexity of the data arrangement;
    ii. complete PITAs;

[10] *Public Governance, Performance and Accountability Act 2013* (Cth) s 12 (definition of 'accountable authority').

[11] *Public Service Act 1999* (Cth) s 7 (definition of 'Agency Head').

[12] *Public Service Act 1999* (Cth) s 13.

iii. complete Data and Analytics Ethical Impact Threshold Assessments;
iv. ensure security and access controls are applied to the data;
v. complete other supporting technical artefacts and records of decisions;
vi. ensure ongoing stewardship is applied; and
vii. regularly review arrangements between parties and risk/issue escalation pathways.

25. ATO staff can seek guidance from the ATO Privacy Officer and OGC on their obligations to assess, advise on and report any potential or actual data breaches, as well as legal advice on whether a use or disclosure of protected taxpayer information or personal information is lawful.
26. The ATO makes public, through its Privacy Policy, detailed information regarding how personal information is collected, used, stored and disclosed,[13] and provides further transparency of its 28 data-matching activities and protocols.[14]
27. These policies and publicly available content are subject to constant review and are regularly updated to ensure currency with legislative changes (notably the privacy reforms), community expectations and operational practices.

Education and training arrangements

28. All ATO employees and contractors must complete assessment based mandatory privacy training before accessing personal information. Mandatory privacy training is completed on commencement with the ATO and annually thereafter.
29. The training incorporates practical scenarios, legislative obligations, data management foundations and ethics, and links to internal policies and external privacy messaging.
30. Completion rates for mandatory training are monitored, and non-conformance is followed up through management processes.

Security of Information

31. The ATO protects personal information through a layered security approach aligned to whole-of-government requirements under the Protective Security Policy Framework (PSPF), including:
    a. ensuring appropriate controls and security classifications of information
    b. comprehensive system access rules for staff concerning access to information, which are reviewed annually
    c. enforcement of the 'need-to-know' principle to ensure ATO staff and contractors only access information required for their role
    d. audit logging and system access monitoring

[13] https://www.ato.gov.au/about-ato/commitments-and-reporting/information-and-privacy/your-privacy

[14] https://www.ato.gov.au/about-ato/commitments-and-reporting/in-detail/privacy-and-information-gathering/how-we-use-data-matching#ato-Currentdatamatchingprotocols

32. Information security controls are aligned with the Australian Government Information Security Manual (ISM) and applied to systems handling personal information, with technical and administrative controls proportionate to data sensitivity, including access controls and encryption where required.
33. Security by design principles are embedded through cyber architecture and system design governance, ensuring privacy and security requirements are addressed upfront in the design, procurement or change of systems rather than retrofitted after implementation.
34. The ATO maintains established cyber security governance, risk management, and assurance arrangements, including conformance reporting and internal and external audit and assurance activities. These activities enable the ATO to validate the ongoing effectiveness of controls and provide assurance to the Accountable Authority[15] (the Commissioner of Taxation) that personal information is appropriately protected.
35. To ensure the integrity of the ATO's systems and reduce the risk of unauthorised access or disclosure of taxpayer information the ATO has robust proof of identity (POI) and proof of record ownership (PORO) practices. The ATO provides comprehensive identity management guidelines and instructions for staff to ensure they verify the identity of a person, or their authorised representative, when attempting to access their information or update or add taxpayer information to ATO records.
36. The ATO has an impersonation scam management capability that allows the ATO to apply protective measures to compromised accounts, to help safeguard personal and tax information and prevent further misuse. More recently, the ATO has introduced further security measures through the ATO app, which allows taxpayers to verify that it is the ATO attempting to contact them, notify users in real time when key changes are made to their ATO account, and provides users with the ability to 'lock' their ATO account if they suspect misuse[16].
37. When the ATO becomes aware that a taxpayer's account may have become compromised, various protective measures will be applied to identify and manage risks of unauthorised access to personal information.
38. The ATO has a range of safeguards and controls in place to ensure that any storage, use, sharing, management and retention of data is appropriate and lawful. The ATO manages its information assets (information, data and records) with transparency and accountability, in accordance with pre-approved destruction authorisations, under the Archives Act 1983.[17]

Notifiable data breaches and cyber incidents

39. The ATO maintains a data breach response plan which sets out processes for identifying, assessing, remediating and notifying potential and actual data breaches.

[15] *Public Governance, Performance and Accountability Act 2013* (Cth) s 12 (definition of 'accountable authority').

[16] https://www.ato.gov.au/online-services/online-services-for-individuals-and-sole-traders/ato-app; https://www.ato.gov.au/media-centre/ato-launches-new-app-feature-to-stop-scam-calls

[17] Division 2 of *Archives Act 1983* (Cth).

40. The number of notifiable data breaches identified since 2022–23 is set out in Table 1 below.

Table 1: Notifiable Data Breaches

Financial year	Number of notifiable data breaches	Method of identification
2022–23	Nil	N/A
2023–24	Nil	N/A
2024–25	1	External Report[18]

41. The ATO conducts regular data breach simulations to strengthen preparedness and continuously improve response arrangements.
42. The ATO's data breach processes form part of a mature and well exercised Business Continuity Management (BCM) response capability that supports enterprise-wide responses to cyber incidents, including those involving data breaches. BCM operates at an enterprise level, coordinating arrangements to ensure continuity of critical services, effective consequence management, timely executive decision-making and clear escalation during high-impact cyber events.
43. BCM is integrated into the ATO's cyber incident, security and crisis response arrangements, including the Cyber Operations Incident Response Plan, Major Incident Management processes, Crisis Communications capabilities and the Continuity Management Team (CMT) framework. During significant cyber incidents, BCM provides centralised coordination, impact assessment, escalation pathways and executive forums to ensure operational, reputational, legal and workforce considerations are managed in parallel with technical response activities.
44. The effectiveness of these arrangements is frequently tested through a regular program of cyber and data breach simulations and exercises, including SES-level and CMT-level scenarios.
45. The ATO maintains established working relationships with external partners, including the National Office of Cyber Security, to support information sharing and whole-of-government coordination during nationally significant cyber events. These connections are exercised through planning, simulations and incident response activities to ensure the ATO can integrate Commonwealth-level situational awareness and response arrangements when required.

Risk, Assurance and Audit arrangements

46. Privacy and taxpayer confidentiality risk is recorded on the ATOs Enterprise Risk Register and compliance is monitored within the ATO Risk Management Framework.

[18] This relates to the unauthorised access of a discrete group of taxpayer records by an ATO employee. The matter was brought to the ATO's attention by state police and out of caution, the ATO proactively notified the OAIC.

47. Controls to mitigate privacy risk include annual mandatory training, system monitoring, access controls, privacy impact assessments, data breach simulation exercises, and the maintenance of comprehensive privacy and information security policies and procedures.
48. Visibility of these risks are provided through reporting to the ATO Executive, ATO Audit and Risk Committee and the Privacy Champion.
49. The ATO conducts regular assurance activities to test privacy controls are operating effectively, such as monitoring staff compliance with mandatory privacy training, conducting annual assurance for PIAs and undertaking annual joint reviews with data exchange partner agencies.
50. As with other public sector bodies, the ATO is subject to external oversight by the OAIC[19], ANAO[20], Commonwealth Ombudsman, however, is also subject to additional oversight by the Taxation Ombudsman.
51. ATO programs and practices are subject to independent, internal oversight by its Internal Audit function. Recently, the ATO's Internal Audit function presented its audit report[21] of the ATO's Data Breach Incident and Response Management, which considered the ATO's management of privacy risks.
52. ATO Internal Audit found the ATO's response to major data breaches is effective, but preparedness is constrained by fragmented risk and continuity arrangements. The ATO is implementing recommendations to strengthen readiness through clearer priorities, risk-based planning and KPIs.
53. As part of the ATO's implementation of Recommendation 16.2 of the *Royal Commission into the Robodebt Scheme*, the ATO is undertaking a joint review with Services Australia to ensure legal compliance with privacy and taxpayer confidentiality in existing or proposed data-matching program protocols between the two agencies.
54. The learnings from the Recommendation 16.2 review will be applied to the ATO's broader data exchanges. Whilst the review is ongoing, the preliminary findings are that improvements need to be made in respect of governance arrangements/documentation, privacy collection notices, ensuring personal information is accurate, up to date, complete and relevant, and clearer processes regarding the destruction of personal information involved in data matching.
55. Oversight of the implementation status of Recommendation 16.2 has been provided by way of updates reported to the Department of Prime Minister & Cabinet.
56. In June 2022, the OAIC published a report of its assessment of Australian Government agencies' compliance with section 15.1 of the APP Code to maintain a PIA register. The OAIC found the ATO to be compliant and did not have any suggestions or recommendations for the ATO.

[19] https://www.oaic.gov.au/privacy/privacy-assessments-and-decisions/privacy-assessments/securing-personal-information-australian-taxation-office,-data-matching-activities

[20] https://www.anao.gov.au/work/performance-audit/governance-of-artificial-intelligence-the-australian-taxation-office

[21] 30 January 2026.

Privacy complaints

57. The ATO has established processes for receiving, managing and resolving privacy complaints. The public can lodge complaints, including privacy complaints, through several channels such as, phone, complaints webform or post.[22]
58. All privacy complaints made to the OAIC are assessed by OGC and are brought to the attention of the Privacy Officer. In this way, trends and risks, if any, are identified and remediated.
59. Complaints to the OAIC remain proportionately small considering the size of the ATO and its activities and data holdings. For the 2024-25 FY, the OAIC finalised 4 complaints in respect of the ATO; 3 which the OAIC decided not to investigate and 1 which was withdrawn.
60. Similarly in the 2023-24 FY, the OAIC finalised 2 complaints in respect of the ATO; 1 which the OAIC decided not to investigate and 1 which was resolved without an admission of privacy interference.

Conclusion

61. The ATO recognises the critical importance of protecting the privacy of individuals and maintaining trust in the public sector.
62. Through strong governance, embedded risk management, comprehensive policies, mandatory training, and assurance processes, the ATO considers its privacy and information security arrangements to be robust and mature.
63. The ATO remains committed to continuous improvement and transparency and will continue to strengthen its privacy practices in line with legislative reform and evolving community expectation. Further information can be provided on request.

[22] https://www.ato.gov.au/about-ato/contact-us/complaints-compliments-and-feedback/complaints-about-the-ato/how-to-lodge-your-complaint