Australian Government
Attorney-General's Department

May 2026

Joint Committee of Public Accounts and Audit

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

Attorney-General's Department Submission

1. Introduction

The Attorney-General's Department (the department) welcomes the opportunity to make a submission to the Joint Committee of Public Accounts and Audit's inquiry into the management of client privacy in the Australian public sector.

This submission outlines the department's role in maintaining a robust legislative and policy framework for privacy protection and information security across the Australian public sector, including through its role supporting the Attorney-General as Minister responsible for:

- the *Privacy Act 1988* (Cth) (Privacy Act), which regulates how Australian Government agencies and certain private sector and not-for-profit organisations handle personal information
- the *Freedom of Information Act 1982* (Cth) (FOI Act), which provides a right of access to government-held information, and
- the *Australian Information Commissioner Act 2010* (Cth) (AIC Act), which established the independent Office of the Australian Information Commissioner (OAIC), Australia's federal regulator for privacy and freedom of information. The OAIC is headed by the Information Commissioner, and also includes the Privacy Commissioner and Freedom of Information Commissioner.

This submission also provides an overview of the department's privacy practices, including its handling of personal information and its privacy governance and capability.

2. Legislative and policy frameworks

2.1 Operation of the Privacy Act

The Privacy Act is the primary legislative framework for the collection, use, disclosure, and storage of Australians' personal data. It contains 13 Australian Privacy Principles (APPs), which regulate the handling of personal information. [1]

The APPs generally apply to most Australian Government agencies, to private sector and not-for-profit organisations with an annual turnover of over $3 million, and some other organisations (collectively, 'APP entities'). [2] As principles-based law, the APPs are designed to regulate APP entities in a flexible way across the information lifecycle. They ensure privacy is protected while enabling APP entities to tailor their personal information handling practices to meet their needs and those of their clients. [3] An act or practice that breaches an APP is an interference with the privacy of an individual. The Information Commissioner has a wide range of enforcement powers to respond to non-compliance with APPs, and may seek civil penalties. [4]

[1] Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not and does not need to be recorded in a material form. Sensitive information, including health information, is a subset of personal information and generally given greater protection under the Privacy Act (*Privacy Act 1988* (Cth), s 6(1)).
[2] Certain Australian Government agencies are excluded from the Privacy Act, including intelligence and national security agencies (Privacy Act s 7). Certain small businesses operators and state authorities and instrumentalities are also prescribed as organisations for the purposes of the Privacy Act under the *Privacy Regulations 2025*.
[3] Explanatory memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth), 52.
[4] Privacy Act s 13.

The Privacy Act recognises that while Australians have a right to privacy, it is not absolute. There may be certain constraints on this right where an individual's privacy must be balanced with other imperatives (for example, where an entity reasonably believes the collection, use or disclosure of personal information is necessary to lessen or prevent a serious threat to life, health or safety of any individual, or to public health or safety).

2.1.1. Australian Privacy Principles

Under APP 1, APP entities are required to take such steps as are reasonable in the circumstances to implement practices, procedures, and systems relating to the entity's functions or activities to ensure the entity complies with the APPs and any relevant APP Code. This includes having a clearly expressed privacy policy that outlines the entity's practices and systems relating to the management of personal information.

An APP entity is not permitted to collect personal information unless the information is reasonably necessary for, or directly related to, its functions or activities unless an exception applies (APP 3), and the entity must take reasonable steps to notify an individual of the collection of their personal information (APP 5). APP 6 provides that an APP entity which holds personal information about an individual can only use or disclose the information for the particular purpose for which it was collected (known as 'the primary purpose') unless an exception applies. Exceptions include:

- where an individual has consented to the secondary use or disclosure
- where an individual would reasonably expect the secondary use or disclosure, and, in the case of sensitive information, it is directly related to the primary purpose of collection, or
- if the secondary use or disclosure is required or authorised by or under an Australian law or a court/tribunal order.

An APP entity which holds personal information must take reasonable steps to protect this information from misuse, interference and loss, as well as unauthorised access, modification or disclosure (APP 11). The type of steps that are reasonable to take to protect information will depend on the circumstances of the entity and the risks associated with the personal information handled by the entity. APP 11 also requires entities to take reasonable steps to destroy or de-identify personal information they hold once the personal information is no longer needed for any purpose for which the personal information may be used or disclosed under the APPs. The APPs impose obligations on agencies and organisations subject to the Privacy Act concerning access to, and correction of, an individual's own personal information (APPs 12 and 13). Individuals also have a right of access to their personal information and to apply for the correction or annotation of their personal information under the FOI Act.

2.1.2. Privacy (Australian Government Agencies – Governance) APP Code 2017

Australian Government agencies must also comply with the *Privacy (Australian Government Agencies – Governance) APP Code 2017* (AGA Code).[5] The AGA Code 'requires agencies to move towards a best practice approach to privacy governance, by ensuring consistent implementation of the key practices, procedures and systems required under APP 1.2'. The AGA Code is designed to contribute to building public trust and confidence in information handling practices.[6]

[5] Ibid pt IIIB, div 2.
[6] Explanatory Statement, *Privacy (Australian Government Agencies – Governance) APP Code 2017*, 1.

A breach of the AGA Code constitutes an interference with the privacy of an individual. The Information Commissioner has a range of enforcement powers to respond to APP entities that do not comply, including investigation powers and access to a range of civil penalties.[7]

Under the AGA Code, an agency must, amongst other requirements:

- have a privacy management plan (PMP)
- have a designated Privacy Officer or Officers
- conduct a privacy impact assessment (PIA) for all high-risk privacy activities, and
- maintain a register of the PIAs conducted and make the register available on its website and regularly review and update its privacy procedures and systems.

A PIA is a written assessment which identifies the impact that an activity or function might have on the privacy of individuals, and makes recommendations for managing, minimising or eliminating those impacts.[8]

2.1.3 Notifiable Data Breaches scheme

The Notifiable Data Breaches scheme (NDB scheme) in Part IIIC of the Privacy Act requires APP entities to notify, as soon as practicable, affected individuals and the OAIC about eligible data breaches. These breaches occur in circumstances where there is unauthorised access to, or disclosure of, personal information and a reasonable person would conclude that the access or disclosure would result in a likely risk of serious harm to any of the affected individuals.[9] If an entity suspects there may have been an eligible data breach, it must complete an assessment to determine whether an eligible data breach has occurred and take reasonable steps to ensure the assessment is completed within 30 days of becoming aware of the circumstances.[10]

If more than one entity jointly and simultaneously holds the same particular record of personal information, an eligible data breach of one entity may also be an eligible data breach of each of the other entities. If one of the entities concerned complies with its NDB obligations under Part IIIC of the Privacy Act, each of the entities is taken to have complied with their obligations. [11] In circumstances where the Information Commissioner is satisfied that an eligible breach has occurred and no notification has been made, the Information Commissioner may give a written direction requiring the affected entity to provide notification of the data breach.[12]

The NDB scheme recognises that technological advancements have facilitated the handling of large amounts of personal information in electronic form which poses an increased risk of data breaches and allows affected individuals to take remedial steps to lessen the potential adverse impacts from a data breach in light of their own circumstances. [13]

To support compliance with the NDB scheme, the OAIC provides advice and guidance to entities and makes information publicly available online. The department also monitors data breaches and engages with government coordination mechanisms in response to data breaches and cyber security incidents where appropriate.

---

[7] Privacy Act s 13, pt III, div 1, pt V.
[8] Ibid s 33D(3).
[9] Privacy Act s 26WE(2).
[10] Ibid s 26WH.
[11] Ibid s 26WK(4), s 26WM.
[12] Ibid s 26WR.
[13] Explanatory Memorandum, Privacy Amendment (Notifiable Data Breaches) Bill 2016, 3.

2.2 Operation of the FOI Act

The FOI Act provides the public the right to access information held by Australian Government ministers and agencies, including for an individual to seek access to their own personal information. The FOI Act also provides individuals with a right to apply to an agency or minister to amend or annotate records of their personal information that are incomplete, incorrect, out-of-date, or misleading.[14] The FOI Act further provides for merits review in respect of decisions on providing access to information, or on the amendment or annotation of records of personal information.[15]

Access to information under the FOI Act is also subject to some limitations, including personal privacy. The FOI Act includes a conditional exemption in respect of documents where disclosure would involve the unreasonable disclosure of personal information of any person (including a deceased person).[16]

2.3 Role of the Office of the Australian Information Commissioner

The OAIC is Australia's independent federal regulator for privacy and freedom of information. Its functions include receiving complaints and conducting investigations into privacy breaches—and pursuing enforcement action where appropriate—and providing guidance and information to regulated entities and the public.

The OAIC is also responsible for overseeing and regulating the public's right to access information. Its functions include the oversight of the operation of the FOI Act, including promoting awareness and understanding of the FOI system, reviewing FOI decisions made by agencies and ministers, and other monitoring, reporting, training, advisory and investigatory functions.

One of the OAIC's regulatory priorities for 2025-26 is strengthening the information governance of the Australian Public Service, including through 'highlighting areas where information handling practices are inadequate and data is not managed appropriately through its lifecycle'.[17]

The OAIC's preferred regulatory approach is to facilitate voluntary compliance with privacy obligations and to work with entities to ensure best privacy practice and prevent privacy breaches'.[18] However, if following investigation the Information Commissioner identifies that there has been an interference with the privacy of an individual, the Privacy Act confers a range of regulatory options which escalate from less serious to more serious options. These includes making a determination that there was an interference with privacy, that an entity must take certain steps to ensure the act or practice is not repeated, and that one or more individuals is entitled to a specific amount of compensation. The Commissioner may also commence civil penalty proceedings in the Federal Court or Federal Circuit and Family Court for an interference with privacy by a regulated entity.[19]

---

[14] See Part V of the FOI Act.
[15] This includes internal review under Part VI and Information Commissioner Review under Part VII of the FOI Act.
[16] See FOI Act, s 47F and s 11A(5).
[17] OAIC, *OAIC regulatory priorities*, (Web Page, 29 July 2024) <https://www.oaic.gov.au/about-the-OAIC/our-regulatory-approach/oaic-regulatory-priorities#section-strengthening-the-information-governance-of-the-australian-public-service>.
[18] OAIC, *Privacy regulatory action policy* (Web Page, 23 June 2025) <https://www.oaic.gov.au/about-the-OAIC/our-regulatory-approach/privacy-regulatory-action-policy>.
[19] Privacy Act s 52, s 80W, s 80U.

3. Department's role in administering privacy and FOI frameworks

3.1 Overview

The department plays a key role in maintaining a robust legislative and policy framework for privacy protection and information security. This includes:

- ensuring legislative frameworks remain fit for purpose, particularly in the digital age, where developing technologies are enabling increased collection, use and disclosure of personal information
- undertaking legislative and policy scrutiny work, advising Commonwealth agencies on how proposed measures can achieve policy objectives while maintaining appropriate protections for personal information and public information access rights, and
- providing legal services related to privacy and freedom of information.

3.2 Ensuring the Privacy Act remains fit for purpose

3.2.1 Recent reform work

The department has supported Government to progress a range of recent reforms to the Privacy Act to ensure it remains fit for purpose in a rapidly changing digital environment.

This includes the *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022* (Privacy Enforcement Act), which significantly increased penalties for serious breaches of privacy under the Privacy Act, incentivising entities to take strong privacy and cyber security measures to protect personal information. Maximum penalties for a serious interference with privacy by a body corporate now are the greater of:

- $50 million
- three times the value of any benefit obtained through the misuse of the information; or
- if the value of the benefit cannot be determined, 30 per cent of a company's adjusted turnover in the relevant period.[20]

The Privacy Enforcement Act provided the Information Commissioner with enhanced enforcement powers to take effective and efficient enforcement action. It also strengthened the NDB scheme to further support the Information Commissioner to assess the particular risk of harm to individuals from an actual or suspected eligible data breach and introduced greater information-sharing powers to ensure regulators are able to work together to take prompt action in relation to data breaches to minimise harm.[21]

From 2020–2022, the department also led the Privacy Act Review which examined whether the scope of the Privacy Act and its enforcement mechanisms remained fit for purpose. The review report made 116 recommendations for legislative and non-legislative reform. The Government responded to the Privacy Act Review on 28 September 2023.[22]

[20] *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022* (Privacy Enforcement Act), sch 1, item 14.
[21] Ibid sch 1, items 18-44.
[22] Australian Government, *Government response to the Privacy Act Review Report* (September 2023) <https://www.ag.gov.au/rights-and-protections/publications/government-response-privacy-act-review-report>.

The department then supported passage of the *Privacy and Other Legislation Amendment Act 2024* (the 2024 Amendment Act), which passed Parliament in November 2024, representing a first tranche of privacy reform following the Government's response to the Privacy Act Review.

Among other matters, the 2024 Amendment Act provided the Information Commissioner with access to a broader range of enforcement options, including new civil penalty provisions and infringement notices for less serious privacy breaches. This addressed a gap whereby the Information Commissioner could previously only seek civil penalties for the most serious or egregious interferences with privacy. The 2024 Amendment Act also triggered the standard monitoring and investigation powers in the *Regulatory Powers (Standard Provisions) Act 2014* (Cth) to support a consistent regulatory approach and to provide the Information Commissioner with modernised powers reflective of a complex digital environment.[23]

To minimise the risk of data breaches and harm arising from cyber incidents, the 2024 Amendment Act clarified the steps—including the implementation of technical and organisational measures—an entity is required to take when protecting personal information (consistent with APP 11).[24]

3.2.2 Ongoing reform work

The Government has committed to delivering a second tranche of reforms to the Privacy Act following passage of the 2024 Amendment Act. The Attorney-General is exploring a balanced package of reforms, including proposals agreed in principle in the Government's 2023 Response to the Privacy Act Review Report, as well as some simplification and deregulatory measures, and measures to enhance the effectiveness of the privacy regulator. Relevant reforms under consideration include updated definitions, and a broad, general requirement for the collection, use and disclosure of personal information to be 'fair and reasonable' in the circumstances.

The proposed 'fair and reasonable' test under consideration would replace the Privacy Act's current requirements with a simplified, principles-based test for information handling that shifts responsibility to protect and manage personal information so that it is shared more evenly between entities and individuals. It is expected that this approach would reduce the overuse of broad and excessive consent requirements. The content and timing of a second privacy reform package is a matter for Government.

Separately, the department agreed to the following recommendations of the Auditor-General Report No. 12 of 2025-26: *Managing the Privacy of Client Information in Services Australia:*

- **Recommendation 2**: The Australian Government consider implementing arrangements to support Services Australia being provided with timely notification of third-party data breaches involving government-related identifiers such as Medicare numbers and Centrelink references numbers.
- **Recommendation 5**: There is limited reporting to the Australian Parliament by Australian Government entities on their compliance with the *Privacy Act 1988.* Entities are not required to report in annual reports on their management of privacy. The Attorney-General's Department, in consultation with the Department of Finance as required, consider advice to the Australian Government on options to improve transparency of entities' compliance with the *Privacy Act 1988.*

[23] *Privacy and Other Legislation Amendment Act 2024* (Cth) (2024 Amendment Act), sch 1, pts 8–14.
[24] Ibid sch 1, pt 5.

The department recognises the importance of ensuring Australians' personal information is managed in accordance with the Privacy Act and is considering these recommendations, including in consultation with the Department of Finance.

3.3 Legislative and policy scrutiny

The department also undertakes scrutiny functions in its administration of the Privacy and FOI Acts. This includes reviewing draft Bills and legislative instruments to assess their impacts on privacy and freedom of information, and advising on how proposed measures can achieve policy objectives while maintaining appropriate protections for personal information and public information access rights.

The Office of Parliamentary Counsel (OPC) refers draft Bills and instruments to the department for review under Drafting Direction 4.2.[25] Where Bills and legislative instruments are referred to the department for scrutiny, the department advises instructing agencies on how to best structure provisions that provide for collection, use, disclosure or storage of personal information in a way that achieves the policy objective while providing privacy protections that are appropriate in the circumstances. Agencies are also advised to include an explanation in explanatory materials, clarifying what information is anticipated to be collected and justifying why this collection is reasonable, necessary and proportionate to achieving a legitimate aim.

The department may be asked to provide advice about policy proposals that are relevant to these matters before a draft Bill or legislative instrument is prepared. These encompass a range of policy issues involving the use of information and data, and appropriate standards of integrity, security and transparency when managing information.

The department is also referred draft and final legal advice where it relates to the interpretation of the Privacy Act and FOI Act from external agencies under section 23 of the *Legal Services Directions 2025*.[26] This consultation is intended to reduce the potential for inconsistent advice and action on legal issues across the Commonwealth, maximise efficiencies and minimise duplication.[27]

3.4 Statutory declaration powers under the Privacy Act

The department supports the Attorney-General in exercising statutory declaration powers under the Privacy Act that enable APP entities to handle personal information in ways that may otherwise not be permitted under the APPs. These declaration powers relate to eligible data breaches and emergencies and disasters.[28]

3.5 Legal services

The Australian Government Solicitor (AGS) Group in the department provides legal advice and services to Australian Government agencies on privacy and information law. This includes advice on the operation of the Privacy Act and the APPs, development of PIAs, managing data breach responses, and representing agencies in court proceedings. AGS plays a key role in supporting compliance with legal obligations, managing risk, and lawful service delivery across government operations.

---

[25] Office of Parliamentary Counsel, *Drafting Direction No. 4.2 – Referral of drafts to agencies* (April 2025) <https://www.opc.gov.au/sites/default/files/2025-05/DD%204.2.pdf>.
[26] *Legal Services Directions 2025* s 23.
[27] Attorney-General's Department, *Guidance Note 3 – Sharing advice within Government* (Website, 2 March 2026) < https://www.ag.gov.au/legal-system/publications/gn-3-sharing-advice-within-government>.
[28] Privacy Act s 26X and pt VIA

4. The department's privacy practices

The department is bound by the Privacy Act and the AGA Code. The department seeks to maintain high standards of personal information handling across all its functions and activities. The department's privacy policy is available at https://www.ag.gov.au/privacy-policy.

4.1 Privacy maturity and risk profile

The department self-assesses its privacy maturity using the OAIC's Privacy Management Maturity Framework, covering 21 attributes across five elements: Governance and Culture; Privacy Strategy; Privacy Processes; Risk and Assurance; and Data Breach Response. The department assesses its privacy risk profile as 'medium', reflecting its functions, policy leadership role for the Privacy Act, reliance on public trust, and the volume and sensitivity of personal information it handles.

4.2 Handling of personal information

The department collects, uses, discloses and stores a broad range of personal information that is reasonably necessary to perform its statutory and administrative functions, including:

- legal casework, including providing legal advice to Commonwealth agencies, international crime cooperation, federal offenders, international family law, private international law, and complaints under United Nations human rights conventions
- regulatory schemes, including the Foreign Influence Transparency Scheme, the Lobbying Register, the Modern Slavery Statements Register, and accreditation of Family Dispute Resolution Practitioners and the management of the register of Marriage Celebrants
- Identity Verification Services, including administration of the Document Verification Service, Face Matching Services and the National Driver Licence Facial Recognition Solution
- programs and initiatives such as legal assistance, grants, contracts and funding agreements, and
- employment and personnel matters relating to staff and contractors.

Collection (APPs 3 and 4)

Personal information is ordinarily collected by the department directly from individuals. In limited circumstances, information may be collected from third parties or publicly available sources, where lawful and appropriate, including where direct collection is unreasonable or impracticable or where required or authorised by law. Sensitive information is generally collected with consent, unless an exception under the Privacy Act applies. The department does not collect information unless it is required for a legitimate departmental purpose.

Use and disclosure (APP 6)

Personal information collected by the department is used and disclosed for the primary purpose for which it was collected. Secondary use or disclosure occurs only where permitted by law, including with consent, where reasonably expected by the individual, or where required or authorised by or under an Australian law or a court/tribunal order.

Anonymity and pseudonymity (APP 2)

Where practicable, individuals may interact with the department anonymously or by using a pseudonym. Identification is required where necessary to perform departmental functions or where it would be impracticable to deal with an individual without confirming their identity.

4.3 Data quality, security and retention

Data quality (APP 10)

The department takes reasonable steps to ensure that personal information it collects, uses or discloses is accurate, up-to-date and complete.

Security and retention (APP 11)

The department applies technical and organisational security controls to protect personal information from misuse, interference, loss and unauthorised access, modification or disclosure. Where personal information is no longer required and is not subject to record-keeping obligations, it is destroyed or de-identified in accordance with the *Archives Act 1983* (Cth) and the Privacy Act.

Access and correction (APPs 12 and 13)

Individuals may request access to, and correction of, personal information held by the department. Requests are managed by the department's Privacy Unit and are subject to appropriate identity verification requirements. Individuals may also lodge complaints with the department if they maintain concerns about the department's handling of their personal information.

4.4 Privacy governance and capability

The department implements the AGA Code through a comprehensive set of governance and capability measures, including:

- maintaining a PMP that outlines measurable objectives and compliance activities. The PMP is reviewed annually to ensure it continues to reflect the department's operating environment, endorsed by the Executive Board and published on the department's website
- PIAs are undertaken for high-privacy-risk initiatives, supported by Privacy Threshold Assessments, standardised PIA templates and proactive engagement to embed Privacy by Design
- designated Privacy Officers and a senior-level Privacy Champion provide oversight and advocacy. The rotating Privacy Champion role promotes enterprise-wide integration while two full-time Privacy Officers provide specialist advice
- mandatory privacy training for all staff on commencement and annually, supplemented by tailored training for higher-risk areas and data breach response, and
- privacy policies, procedures and APP 5 collection notices are reviewed regularly using plain English and standardised templates and tested with business areas for clarity and consistency.

4.5 Privacy by Design

The department applies a Privacy by Design approach by embedding privacy considerations into policy development, system design and service delivery. Privacy risks are assessed through PIAs, and controls are applied to limit the use of personal information, particularly in the context of emerging technologies, including AI-enabled tools.

4.6 Responding to data breaches

The department is subject to the NDB scheme established by the Privacy Act and maintains a Data Breach Response Plan that sets out clear procedures for identifying, assessing, containing and responding to data breaches, including notification requirements. The Data Breach Response Plan is regularly reviewed and a simulation exercise is conducted annually. The department seeks to protect the personal information it handles from data breaches through governance and assurance arrangements, staff training, access controls, and contractual arrangements with third-party service providers.