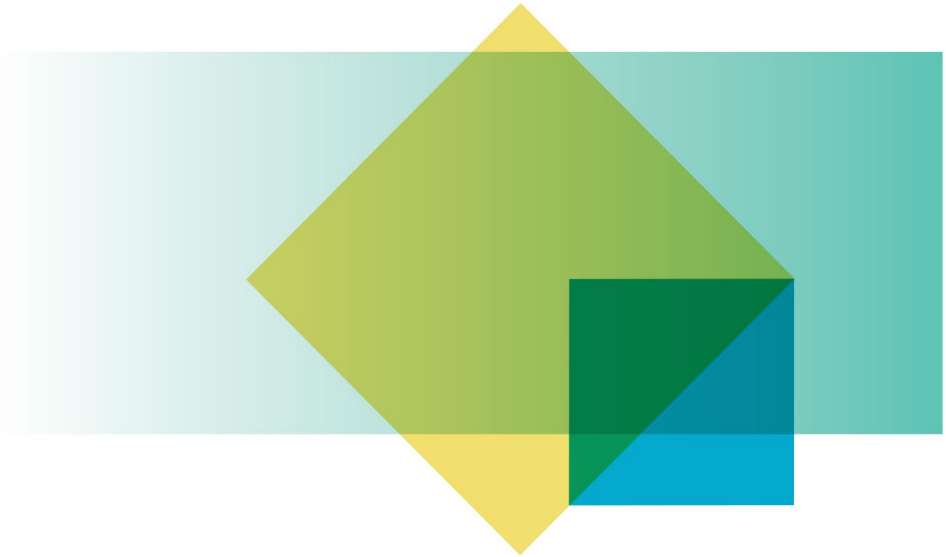
Australian Government
Office of the Australian Information Commissioner

Joint Committee of Public Accounts and Audit inquiry into the management of client privacy in the Australian public sector

Submission by the Office of the Australian Information Commissioner



Elizabeth Tydd
Australian Information Commissioner

Carly Kind
Australian Privacy Commissioner

5 May 2026

OAIC

May 2026

Introduction

The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to provide this submission to the Joint Committee of Public Accounts and Audit for the purposes of its inquiry into the management of client privacy in the Australian public sector.

As an independent statutory agency, the OAIC regulates privacy and freedom of information (FOI) under the Commonwealth *Privacy Act 1988* (Privacy Act) and the *Freedom of Information Act 1982* (FOI Act), respectively, and has specific functions under the *Australian Information Commissioner Act 2010* (AIC Act) relating to access to government information.[1] In addition to these three principal Acts, the OAIC also has regulatory and advice responsibilities conferred under other primary and subordinate legislation, including with respect to privacy.[2]

The requirements on Australian Government agencies under the Privacy Act are supplemented by further obligations imposed through the Australian Government Agencies Privacy Code, which is a binding legislative instrument. In particular, the Code imposes additional specific requirements in relation to Australian Privacy Principle (APP) 1.2 to move towards a best practice approach to privacy governance to help build a consistent, high standard of personal information management.

Government agencies are increasingly handling larger volumes of personal information, and their interactions with the Australian community are occurring more commonly via online platforms.

The Australian Government's 'tell us once' approach, introduced in the *Regulatory Reform Omnibus Act 2025* facilitates greater sharing of information, including sensitive information such as healthcare identifiers, between Government agencies with the intent of reducing red tape, improving efficiency and streamlining user experience.

In addition, the settings and method for delivering certain Government programs also allow for increased capture and sharing of personal and sensitive health information. For example, the recent amendments to the *My Health Records Act 2012* require certain health information to be shared to the My Health Record system by default with limited exceptions.[3] The reforms also provide for additional records to be uploaded to the My Health Records system, with rules to implement sharing by default for prescribed diagnostic imaging and pathology services.

The increasing expansion of AI use by government gives rise to a number of risks and considerations from a privacy perspective. Given that Government agencies have access to highly sensitive personal data, they must be aware of the heightened risk of misuse of personal information in the training of AI. More broadly, agencies should ensure that their privacy policies communicate how personal information is collected, used and retained, including in and by AI systems. Transparency of how personal information is processed is essential to promote public trust and confidence in the use of AI by public institutions.

---

[1] The functions of the OAIC are set out in the AIC Act, see relevantly: section 7 (Definition of information commissioner functions), section 8 (Definition of freedom of information functions) and section 9 (Definition of privacy functions).

[2] The OAIC's regulatory and advice functions derive from 39 statutes and subordinate instruments. For example, in addition to the functions conferred under the Privacy Act, the OAIC also has specific regulatory functions with respect to privacy in relation to the operation of the My Health Records system and Health identifiers.

[3] The sharing by default reforms come into effect from 1 July 2026. The limited exceptions include where a consumer does not have a My Health Record, or where the consumer requests that the information is not uploaded to their record.

This transparency is also supported by agencies' obligations under the Information Publication Scheme (IPS)[4] under which they must publish operational information online. In January 2026, the OAIC published a report on *Automated decision-making (ADM) and public reporting under the FOI Act*[5] which identified opportunities for agencies to improve transparency in the use of ADM and highlighted the positive impact IPS obligations have in ensuring that transparency and accountability of actions and decision are improved in the APS.

The Australian community has a heightened expectation that the public sector will set the benchmark for information governance, particularly as the delivery of government services becomes more digital. Based on the preliminary results from the OAIC's 2026 Australian Community Attitudes to Privacy Survey, around 68% of Australians have trust in Australian Government agencies to protect and appropriately use personal information. Australians appear willing to share information in public-interest contexts, but expect transparency, disciplined stewardship, clear accountability, and strong safeguards where government decisions affect rights and entitlements.[6]

That expectation becomes even more pronounced in relation to AI and automated decision-making. Australians hold government to the highest standard for responsible AI use which reinforces the importance of robust and transparent governance arrangements before high impact tools are deployed.[7]

There are extant protections provided under statutes including the FOI Act that ensure that the right to access both personal and non-personal information is protected notwithstanding government's outsourcing of service provision and its acquisition and deployment of technological solutions to inform decision-making or deliver services.[8] The OAIC is increasingly demonstrating expertise in reconciling, promoting and guiding government and non-government entities to uphold these legislated rights. In this context it is important to understand the mingling of personal and non-personal data that will occur in the use of information and set effective regulatory expectations that will also promote productivity particularly in the treatment of sensitive personal information.

The OAIC's posture and authority is informed by an appreciation of technology related harms impacting the economy and individuals. The scale of the data being processed can increase the risk of disclosure of personal information through data breaches and cyberattacks.

In the 2025-26 financial year to 30 April 2026, the Australian Government sector was the fourth highest sector for privacy complaints received by the OAIC (behind health services, social media and finance (including superannuation)) at 375 (representing approximately 9% of total privacy complaints received in the period). The top issues by number of complaints were APP 6 - Use or disclosure (113 complaints), and APP11 – Security of Personal Information (68 complaints).

[4] About the Information Publication Scheme | OAIC

[5] Australian Information Commissioner highlights improved transparency and integrity for government agencies in automated decision-making | OAIC

[6] Preliminary Findings Australian Community Attitudes to Privacy Survey 2026.

[7] Ibid.

[8] FOI Act, s 6(c)

The Australian Government sector was the sixth highest sector for notifiable data breach notifications to the OAIC, with 62 data breach notifications received to 30 April 2026 in 2025-26 (representing 6% of NDBs received in the period). This has reduced from 143 in the same period for the previous year (where the Australian Government had the second highest amount as a sector). Malicious or criminal attacks remain the largest source of data breaches in the Australian Government sector, followed by human error.

The increased handling of personal information by and between Government agencies, along with the changing technology landscape, requires a continued focus on improving transparency and accountability and record keeping by Government agencies, as well as an ongoing capability uplift across the public sector to mitigate the increased risks associated with breaches, malicious actors and cyber security.

Frameworks used to identify and manage privacy risks, and meet the requirements of the Privacy Act

Privacy Act: APPs, NDB Scheme and the Privacy Code

The *Privacy Act 1988* (the Privacy Act) provides the legal framework under which Australian Government agencies covered by the Privacy Act must operate to protect personal information. As effectively covered in the Managing the Privacy of Client Information in Services Australia audit report (the Services Australia report) (paras 1.3-1.9), the Privacy Act provides protections to personal information through:

- the Australian Privacy Principles (APPs), which govern standards, rights and obligations around the handling of personal information
- the Notifiable Data Breaches Scheme, which governs mandatory reporting of data breaches
- and the Australian Government Agencies Privacy Code, which sets out specific requirements and key practical steps that agencies must take as part of complying with Australian Privacy Principle 1.2 (APP 1.2) (see paras 2.1-2.3, 2.11 of the Services Australia report).

Privacy protections outside the Privacy Act

In addition to the Privacy Act, explicit privacy protections in a number of other acts and legislative instruments regulate Government agencies' management of personal information. Examples include the *My Health Records Act 2012, Digital ID Act 2024, Data-matching Program (Assistance and Tax) Act 1990* and the Privacy (Tax File Number) Rule 2015.

In addition to the regulatory role the Information Commissioner has under the Privacy Act, the Information Commissioner has specific oversight and regulatory roles in relation to a number of these other obligations on Government agencies, including regulating with specific enforcement powers the privacy aspects of the My Health Record system[9], the Digital ID system and the Consumer Data Right scheme.

[9] My Health Records (Information Commissioner Enforcement Powers) Guidelines 2026

The Information Commissioner also has the function of reporting to the Attorney-General on any matter that relates to the Government's policy and practice with respect to the collection, use, disclosure, management, administration or storage of, or accessibility to, information held by the Government, and the systems used, or proposed to be used, for these activities.[10]

Notifiable Data Breaches scheme

Under the Notifiable Data Breaches (NDB) scheme agencies covered by the Privacy Act must notify affected individuals and the OAIC when a data breach is likely to result in serious harm to an individual whose personal information is involved. The OAIC publishes information about the operation of this regulatory scheme in its Annual Report, and via the NDB Dashboard on the OAIC website.

Regulatory tools to identify and manage risk

The OAIC has a range of regulatory tools currently available to assist and encourage agencies to identify and manage privacy risks and to identify and respond to non-compliance.

Regulatory guidance material

The OAIC has a suite of guidance material available to support Government agencies in meeting their privacy obligations, including best practice information and templates and assessment tools.

Regulatory approach

The OAIC's regulatory approach uses both encouragement and deterrence to promote and protect privacy and information access rights. We apply a proactive and harm-focused approach to prioritise our efforts. We take regulatory action to encourage and support compliance by regulated entities and to address high-risk matters with the greatest potential for harm. Recent examples of the OAIC's regulatory action against Government agencies include the determinations in *'ATQ' and CEO of Services Australia (Privacy) [2025] AICmr 19* (23 January 2025) and *'WP' and Secretary to the Department of Home Affairs (Privacy) [2021] AICmr 2* (11 January 2021).

The OAIC has also articulated its approach to regulating privacy protection in the My Health Record system through the My Health Records (Information Commissioner Enforcement Powers) Guidelines 2026. The purpose of these guidelines is to promote transparency in the Information Commissioner's processes, given the Information Commissioner's important role in relation to the My Health Record system. Regulatory collaboration has underpinned our endeavours to date and increasingly our work adopts a co-regulatory approach with the Australian Digital Health Agency (ADHA).

A program of work to assess compliance in this expanding health service is also being delivered by the OAIC to address the risks associated with this important health service offering. Promoting trust and productivity are central to the OAIC's regulatory role in this growing sector.

[10] *Australian Information Commissioner Act 2010*, section 7.

Regulatory priorities

The OAIC regulatory priorities for 2025–26 ensure that the OAIC's resources are focused on the prevention of privacy harm and upholding the community's access to information rights in the areas of greatest impact and concern. Strengthening the information governance of the Australian Public Service is one of the OAIC's four areas of regulatory focus for 2025-26.

Opportunities to improve transparency, accountability and uplift privacy capability in the APS

The OAIC has identified a need for increased transparency, accountability and privacy capability uplift across the APS to maintain trust and confidence in Government agencies as they engage in opportunities to streamline service delivery and increase their efficiency through increased data sharing, automated decision making and AI.

Transparency and accountability

The Services Australia report highlighted the limited reporting requirements of Australian Government agencies regarding their compliance with the *Privacy Act.* The OAIC supports opportunities to increase transparency regarding Government management of personal information, including recommendation 5 directed at the Attorney-General's Department in consultation with the Department of Finance.

Opportunities to improve the use of data and transparency relating to Government agencies' compliance with the Privacy Act is a priority for Commissioners at the OAIC. The OAIC already publishes a dashboard on notifiable data breaches, providing a publicly accessible interactive presentation of available data. This was created to help reporting entities and stakeholders understand the volume of data breaches reported to the OAIC, the number of people affected, causes and sectoral trends. A similar dashboard has been developed for FOI statistics. It serves a productivity and efficiency purpose for both the regulator and regulated entities. Importantly public availability serves accountability and transparency and ultimately fosters trust in government.

The OAIC is investigating opportunities to expand the publicly available information to include a dashboard for Privacy Act compliance. The purpose of this would be to increase transparency around the number and type of privacy complaints made to Government agencies and to uplift agency accountability. The OAIC does not currently have a relevant power to request such information from regulated entities through non-cohesive mechanisms, nor do entities have any obligation to provide complaint data to the OAIC – the OAIC therefore recommends the introduction of such requirements to support the transparency of personal information management.

Transparency around compliance with privacy obligations will become increasingly important as agencies embed automated decision making and the use of AI into operations. The OAIC has actively applied extant legislative provisions and provided statutory guidance to maximise transparency in the use of ADM.

In January 2026, the OAIC's *Automated decision-making (ADM) and public reporting under the FOI Act*[11] report identified opportunities for agencies to improve transparency in the use of ADM and highlighted the positive impact IPS obligations have in ensuring that transparency and accountability of actions and decision are improved in the APS. The OAIC is currently consulting on amendments to Part 13 of the FOI Guidelines: Information Publication Scheme, which seek to implement recommendations from the January report.

In response to AGD's consultation paper *Use of automated decision making by government,* the OAIC recommended the Government introduce an express obligation for agencies to proactively publish information about the circumstances when ADM is in use, including an adequate description of the type of system in use, its purpose and how it operates (including the types of decisions for which it is used), the legislative basis for the decision and any policies relied upon, as well as the assurance processes in place to ensure that the system is being used lawfully.[12]

Given the additional privacy and information access risks associated with the expanded use of AI in Government agencies the OAIC recommends a notification requirement for AI related breaches which would apply to Government agencies, similar to the NDB notification scheme. This would support regulators to track and provide a more immediate co-ordinated response harms identified in the use of AI systems and treatments applied by agencies. This approach would also facilitate an integrated approach to AI regulation and harm - informing regulatory approaches which would also provide guidance to industry and government. A transparent approach to the potential privacy and access harms involved in the use of AI will in turn increase trust and confidence in the deployment of AI by Government agencies.

Improved reporting of third-party data breaches

The OAIC agrees in principle it would be beneficial for Services Australia to be notified of relevant third-party data breaches to enable it to act to prevent future breaches and carry out its functions, as outlined in recommendation 2 of the Services Australia report. Such arrangements may require legislative reform, which is a matter for Government.

If a new reporting obligation is to be imposed, it will be necessary to specify the entities to which the requirement applies and the threshold for notification. For example, consideration should be given to whether the obligation rests with third parties to directly notify Services Australia. The OAIC is not notified of all data breaches involving Services Australia or individual identifiers. The Notifiable Data Breaches scheme only requires entities regulated under the Privacy Act to notify the OAIC if a data breach is likely to result in serious harm to an individual.

[11] Australian Information Commissioner highlights improved transparency and integrity for government agencies in automated decision-making | OAIC

[12] AGD consultation paper – Use of automated decision making by government | OAIC

Uplift across the APS

Proposed NDB self-assessment tool

As part of the OAIC striving to be more efficient in its use of resources and its ability to be responsive to the quantity of data breaches reported, it has proposed an expansion to pilot a quick-response self-assessment tool to assist entities to understand how to comply with the NDB requirements. The self-assessment tool would reduce the regulatory response burden for reporters.

Intelligence gained through NDB and other potential notification requirements

The OAIC is investigating additional case management approaches to promote the efficiency and effectiveness of the NDB scheme including our response to community enquiries and complaints that arise through large scale breaches and drive increasing case numbers in the OAIC. Measures include investing in technology to deploy smart forms and chat bots to guide impacted individuals to the options available to them and promote to the greatest degree possible early and effective resolutions through the active engagement of respondent entities.

Privacy uplift tools

As noted above, the OAIC has a suite of guidance material available to support Australian Government agencies. Of particular relevance to uplifting privacy practices, the OAIC's Privacy Foundations self-assessment tool[13] has been designed to assist entities to embed a culture of privacy, and to establish or improve privacy practices, procedures and systems. Similarly, the interactive privacy management plan tool[14] has been designed to assist Australian Government agencies to assess the current state of the privacy practices and set privacy goals and targets.

Privacy Awareness Week

The May 2026 Privacy Awareness Week (PAW) theme is: ***Trust is built* here. In every privacy complaint. In every resolution**. This year's campaign focuses on strengthening privacy dispute resolution practices and building public confidence in how personal information is handled. It includes the release of a privacy complaint checklist to help entitles manage complaints in a structured, fair, accessible and timely way.[15]

This year's theme coincides with OAIC updating its approach to privacy complaints in line with a shift towards a greater focus on enforcement, ensuring we can resolve matters in a way that will result in meaningful change. The new approach places greater expectation on entities to attempt to resolve the complaint prior to it reaching the OAIC.[16]

[13] Privacy Foundations self-assessment tool | OAIC

[14] Interactive privacy management plan | OAIC

[15] Checklist for privacy dispute resolution

[16] See Handling privacy complaints – a new approach for a new era | OAIC

Privacy decisions

In addition to uplift tools, the OAIC continues to publish privacy assessments and privacy decisions (including determinations) which provide further guidance and precedent on privacy compliance for entities, including Australian Government agencies.[17] Recent determinations have focused on over-collection of personal information, unlawful use of personal information for secondary purposes and failure to secure personal information. These findings are relevant to both private and public sector entities.

Recent litigation outcomes including the first case in which a civil penalty has been imposed under the Privacy Act have a strong deterrent impact and the OAIC is increasingly focused on utilising the full range of its regulatory powers.

Australian Government Agencies Privacy Code

The Australian Government Agencies Privacy Code (the Code) was registered on 27 October 2017 and commenced on 1 July 2018.

The Code applies to all Australian Government agencies subject to the Privacy Act (except for Ministers). It is a binding legislative instrument under the Act.

The Code sets out specific requirements and key practical steps that agencies must take as part of complying with Australian Privacy Principle 1.2. It requires agencies to move towards a best practice approach to privacy governance to help build a consistent, high standard of personal information management across all Australian Government agencies.

The Code enhances existing privacy capability within agencies, builds greater transparency in information handling practices, and fosters a culture of respect for privacy and the value of personal information. The Code therefore symbolises the commitment of Australian Government agencies to the protection of privacy, and helps build public trust and confidence in personal information handling practices and new uses of data proposed by agencies.

The Code sunsets in 2028. In considering the Code going forward the OAIC will seek to identify and consult on key measures to strengthen privacy governance and transparency in Government agencies to align with contemporary community expectations and our changing technological environment. This includes an opportunity to emphasise the need for major project budgets to factors in the cost of conducting a privacy impact assessment at the project initiation phase.

AI guidance for Government Agencies

The OAIC is currently developing holistic (privacy and FOI) guidance materials to support Government use of AI. These respond to feedback from Government agencies about the need for more tailored and practical guidance for APS officers following the launch of the AI Plan for the Australian Public Service 2025. These materials will supplement the OAIC's existing privacy AI guidance for all entities which deals with developing and training generative AI models, and the use of commercially available AI products.

[17] Privacy assessments and decisions | OAIC.

Data matching – Voluntary Guidelines

Recommendation 4 of the Services Australia report recommends the Australian Government review existing data-matching activities undertaken by Services Australia and other government entities to assess whether the current frameworks — the *Privacy Act 1988*, the *Data-matching Program (Assistance and Tax) Act 1990*, and the voluntary Guidelines on data matching in Australian Government administration — are appropriate for use with contemporary data-matching and information-sharing practices and provide sufficient transparency and accountability.

The OAIC's Guidelines on data matching in Australian Government administration (Guidelines) were first issued in 1992. The Guidelines are voluntary and represented the OAIC's view on best practice with respect to undertaking data matching activities at that time.

However, the privacy landscape, including the OAIC's regulatory approach and digital environment, has changed significantly since the Guidelines were issued and the OAIC has also adapted it's regulatory approach over this time. The current complex digital environment requires a proactive contemporary approach to regulation.[18]

The OAIC is currently reviewing the voluntary Guidelines with a view to retiring the Guidelines subject to consultation with relevant agencies. A renewed approach will focus the OAIC's support directly on agencies' mandatory obligations, providing clarity and reducing overlap and thereby promote productivity and effectiveness together with enhanced compliance.

[18] Annual report highlights OAIC's work on privacy and information access rights and strengthened regulatory approach | OAIC