11 November 2025

Legal briefing

Privacy in government transactions

This Legal briefing is intended to assist Commonwealth agencies to identify and manage privacy issues that may arise in the course of a government transaction (such as a procurement).

Commonwealth agencies are subject to privacy obligations under the *Privacy Act 1988* (Cth), Australian Privacy Principles, and the Privacy (Australian Government Agencies – Governance) APP Code 2017.

AGS has developed a checklist of matters that Commonwealth agencies should consider in transactions that may involve the handling of personal information.

The legislative framework for privacy

Privacy Act

Commonwealth agencies are subject to obligations relating to the collection, use, storage and disclosure of personal information under the *Privacy Act 1988* (Cth) (Privacy Act) and the Australian Privacy Principles (APPs) in Sch 1 to the Privacy Act.

Privacy Code

The Privacy (Australian Government Agencies – Governance) APP Code 2017 (the Privacy Code) further sets out specific requirements agencies must comply with. Importantly, the Privacy Code includes the requirement for agencies to conduct a Privacy Impact Assessment (PIA) for any high privacy risk project.

Eligible data breaches

Part IIIC of the Privacy Act sets out the requirements for agencies to notify affected people and the Office of the Australian Information Commissioner (OAIC) when there has been an eligible data breach. Such a data breach involves personal information that is likely to result in serious harm to an individual. In a government transaction, an eligible data breach could occur where for example:

- a database containing personal information managed by a contracted service provider is hacked
- during the course of the transaction, personal information is mistakenly sent to the wrong recipient.

Other specific legislation

In some circumstances, other legislative obligations will also apply. For example:

- there may be statutory regimes or secrecy provisions that apply to personal information (e.g. health information protected under the *My Health Records Act 2012* (Cth), and secrecy provisions protecting Medicare, the Pharmaceutical Benefits Scheme, and Australian Taxation Office data)
- a contracted service provider or other third party may be required to comply with state or territory privacy legislation.

This publication does not discuss the application of other specific legislation, rules or secrecy provisions.

When can privacy issues arise in a government transaction?

Given the obligations under the Privacy Act and the Privacy Code, privacy should be an ongoing consideration throughout the life of any Commonwealth project, including government transactions like procurements.

All Commonwealth agencies should assess when and how personal information will be handled during a project, as this can trigger certain legislative obligations under the Privacy Act (such as the requirement to conduct a PIA).

Examples of types of government transactions where privacy issues commonly arise include:

- ICT procurements that involve new or changed ways of collecting or handling personal information (e.g. new surveillance software or new handling of customer or employee data)
- digital transformation procurements, such as uplifting internal systems or introducing new software that involve handling personal information
- data exchange agreements and deeds, including collaborative agreements between different agencies
- implementation of Artificial Intelligence (AI) technologies, including for use in automated decision-making processes
- arrangements in relation to data matching
- procurement of service providers to perform functions or provide services where they interface with individuals (e.g. the general public, agency staff or particular sections of the community)
- arrangements with service providers that involve the movement of data (e.g. from an onsite server to the cloud).

How to identify privacy risks in a transaction or arrangement

Privacy threshold assessments

A Privacy Threshold Assessment (PTA) is a preliminary assessment as to the level of privacy risk involved in a project. Agencies may conduct a PTA to identify whether a project meets the threshold of a 'high privacy risk project' that may require a PIA under the Privacy Code.

Privacy impact assessments

Section 12(1) of the Privacy Code requires agencies to conduct a PIA for all 'high privacy risk projects'.

A project may be a high privacy risk project if the agency responsible for the project reasonably considers that it involves any new or changed ways of handling personal information that are likely to have a significant impact on the privacy of individuals.[1]

Guidance from the OAIC provides that an impact on the privacy of individuals will be 'significant' if the consequences of the impact are considerable, taking into account their nature and severity.[2]

While the status of a project as a 'high privacy risk project' will depend on the circumstances of the particular project, factors that might indicate a project meets this definition include:

- the project involves the handling of 'sensitive information' (as defined in s 6(1) of the Privacy Act e.g. a person's health information or information about a person's criminal record)
- an agency proposes to disclose personal information collected as part of the project to another agency or another third party
- an agency proposes to use personal information collected for one purpose for a new or different purpose

- the project could have a serious or meaningful consequence for an individual or group of individuals (e.g. because it may deny access to benefits or services)
- the project uses personal information as part of automated decision making, particularly if the automated decision will affect a person's rights and entitlements
- collection of information as part of the project might create a 'honey pot' of information, a large amount of information about lots of individuals or entities being collected and stored in one place.

The OAIC provides useful guidance[3] on screening factors that point to a high privacy risk.

It is best practice to conduct a PIA as early as possible

A PIA identifies the risks and potential impact a project may have on the privacy of individuals and outlines recommendations to manage, minimise, or eliminate such risks and potential impacts.[4]

As such, a PIA is often most useful when an agency conducts the assessment at an early stage of a project. For example, by conducting a PIA once an agency has determined its minimum viable product, the agency can make changes and address the recommendations set out in the PIA before conducting substantial work to implement the project.

If there are substantial changes in the handling of personal information throughout the life of the project, it may be appropriate for the agency to conduct another PIA.

Agencies may also benefit from obtaining targeted privacy advice on specific privacy risks for projects that are low or medium privacy risk.

Mitigating privacy risks in contractual arrangements

Section 95B of the Privacy Act requires agencies entering into a Commonwealth contract[5] to take contractual measures to ensure that a service provider does not do an act, or engage in a practice, that would breach an APP if done or engaged in by the agency itself. Ordinarily, Commonwealth contracts will prescribe an express requirement for a service provider to comply with, or not to breach, the APPs.

In addition, agencies can address project specific privacy risks (including those identified in a PIA or PTA) through contractual arrangements. The specific contractual measures will depend on the nature of the project, but measures could include:

- obligations on the service provider's subcontractors to comply with the Privacy Act and the APPs, and requirements that subcontractors implement specific safeguards to ensure compliance with the APPs
- a requirement for the service provider and any subcontractor to access, use and disclose personal information for the purpose of delivering services under the contract only
- a requirement for the service provider's personnel to execute an acknowledgement or deed of confidentiality, and/or hold a certain level of security clearance, before obtaining access to information
- a prohibition on storing or transmitting information outside of Australia, or only in certain approved ways
- an obligation that the service provider and their systems comply with specific data security[6] and cyber security standards or requirements,[7] including to de-identify certain personal information
- obligations to follow specific processes and requirements in responding to a suspected eligible data breach
- a requirement to notify the Commonwealth if an overseas authority requests access to the data
- obligations related to the use of AI[8]
- a requirement to implement measures to guard against serious invasions of privacy[9]
- robust audit and access rights to enable the Commonwealth to monitor the service provider's compliance with privacy obligations
- incorporation of any agency-specific privacy management practices, procedures and/or systems (e.g. obtaining consent from individuals, giving privacy notices, handling unsolicited information, processing access and amendment requests).

Additionally, when drafting liability and indemnity provisions, agencies should ensure they consider potential losses arising from any breach of privacy-related obligations by a service provider, or any third-party claims arising from a privacy or other data breach incident.

Summary

We set out below a useful 'checklist' for agencies to consider during the planning phase of any project.

Step 1: Identify if your project, arrangement or transaction involves privacy issues

- Does the project involve new or changed ways of handling personal information?
- Consider whether handling of information is subject to other legislative regimes (e.g. health or insurance data, Information Commissioner rules, statutory secrecy provisions, or any state or territory privacy legislation applicable to service providers).

Step 2: Conduct any privacy assessments in a timely manner

- If yes at Step 1, conduct a PTA to determine whether the project is a 'high privacy risk project'.
- If the project is 'high privacy risk', conduct a PIA.
- If not 'high privacy risk, consider whether to obtain more limited privacy advice on specific risks raised by the project.

Step 3: Consider how to address privacy risks in contractual arrangements

- Consider what measures to include in project requirements and contractual arrangements to mitigate the privacy risks for the specific project.
- For example, reflect recommendations from the PIA or any other privacy advice in the project requirements and contractual arrangements.

Notes

1 Section 12(2) of the Privacy Code.

2 When do agencies need to conduct a privacy impact assessment? | OAIC, scroll down to Part 2: Determining whether there is the potential for a 'high privacy risk project'.

3 See also the OAIC's privacy threshold assessment template.

4 Privacy Act, s 33D(3).

5 'Commonwealth contract' means a contract, to which the Commonwealth or an agency is or was a party, under which services are to be, or were to be, provided to an agency: Privacy Act, s 6(1). Services provided to an agency include services that consist of the provision of services to other persons in connection with the performance of the functions of the agency: Privacy Act, s 6(9).

6 For example, the Information Security Manual and the Protective Security Policy Framework. The Hosting Certification Framework may also be relevant, depending on the nature of the arrangement.

7 For guidance on the Digital Transformation Agency's cyber risk model clauses and management of cyber risks in ICT procurements, read *Cyber risk model clauses* [PDF 280KB] (AGS Legal update no. 330).

8 For guidance on the Digital Transformation Agency's AI model clauses and management of risks arising in the procurement of AI systems, read *Artificial Intelligence (AI) model clauses* [PDF 436KB] (AGS Legal update no. 327).

9 See Privacy Act, Sch 2 (Statutory Tort for Serious Invasions of Privacy).

We can help

AGS has experience in preparing PIAs, PTAs, and other privacy related advice. We also have experience in drafting contractual arrangements in projects with specific privacy and data management risks. We can assist you throughout different stages of your agency's project to ensure compliance with your agency's legislative obligations and facilitate better practice in handling personal information.

For further information please contact:

Eamon Holley
Senior Executive Lawyer
T 07 3360 5778 **M** 0409 305 063
eamon.holley@ags.gov.au

Melissa Gangemi
Senior Executive Lawyer
T 03 924 21329 **M** 0458357145
melissa.gangemi@ags.gov.au

Meg Wootten
Senior Lawyer
T 02 6253 7097
meg.wootten@ags.gov.au

Eilish Rolland
Senior Lawyer
T 02 6253 7020
eilish.rolland@ags.gov.au

Francesca Castandiello, Lawyer, assisted with the production of this publication.

Offices

Canberra	4 National Circuit, Barton ACT 2600
Sydney	Level 10, 60 Martin Place, Sydney NSW 2000
Melbourne	Level 34, 600 Bourke Street, Melbourne VIC 3000
Brisbane	Level 33, 300 George St, Brisbane QLD 4000
Perth	Level 21, 2 The Esplanade, Perth WA 6000
Adelaide	Level 5, 101 Pirie Street, Adelaide SA 5000
Hobart	Level 8, 188 Collins Street, Hobart TAS 7000
Darwin	Level 10, TIO Centre, 24 Mitchell Street, Darwin NT

www.ags.gov.au

General enquiries and subscriptions:
T 02 6253 7246
E publications@ags.gov.au

ISSN 1443-9549 (Print)
ISSN 2204-6550 (Online)

Client Services 078–2025 11/25