COUNTRY COMPARATIVE GUIDES 2022

The Legal 500 Country Comparative Guides

Australia

DATA PROTECTION & CYBER SECURITY LAW

Contributing firm

Gilbert + Tobin

Simon Burns

Partner | sburns@gtlaw.com.au

Melissa Fai

Partner | mfai@gtlaw.com.au

Rebecca Dunn

Partner | rdunn@gtlaw.com.au

Mark Ferguson

Lawyer | mferguson@gtlaw.com.au

This country-specific Q&A provides an overview of data protection & cyber security law laws and regulations applicable in Australia.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

AUSTRALIA
DATA PROTECTION & CYBER SECURITY LAW

1. Please provide an overview of the legal and regulatory framework governing data protection and privacy in your jurisdiction (e.g., a summary of the key laws, who is covered by them, what sectors, activities or data do they regulate, and who enforces the relevant laws). Are there any expected changes in the data protection and privacy law landscape in 2022-2023 (e.g., new laws or regulations coming into effect, enforcement of any new laws or regulations, expected regulations or amendments)?

In Australia, data protection and privacy are principally regulated by the federal *Privacy Act 1988* (Cth) (**Privacy Act**). The Privacy Act regulates the collection, use, storage and disclosure of personal information by private sector organisations (with some exceptions) and federal government agencies (but not state agencies). In particular, the Privacy Act sets out 13 Australian Privacy Principles (**APPs**) which set out specific obligations in respect of personal information. The Privacy Act also contains credit reporting obligations which apply to the handling of credit information about individuals by credit reporting bodies, credit providers and some other entities.

The Privacy Act applies to the handling of personal information by private sector organisations generally, however, organisations with aggregate group turnover of less than AUD3 million are not covered by the Privacy Act unless they are: (i) a private sector health services provider; (ii) a business that sells or purchases personal information; (iii) a credit reporting body; or (iv) a contracted service provider for a federal government agency.

The Privacy Act is currently the subject of proposed reform. Please see item 40 for further details.

There are a range of other laws in Australia, both at the federal and state/territory level, which impact data protection. These include:

- state and territory privacy legislation, applying to personal information held by government agencies and private sector contractors to Government agencies (for example, the *Privacy and Personal Information Protection Act 1988* (NSW)). State and territory regulators administer such legislation;
- in New South Wales (NSW), Victoria (Vic) and the Australian Capital Territory (ACT), specific privacy legislation relating to health information and health records, applying to health information collected, used and disclosed by public sector agencies (based in NSW, Vic or the ACT) or private sector organisation that is a health service provider, or that otherwise collects, holds or uses health information;
- federal law requiring telecommunications carriers and carriage service providers to capture and retain certain information about communications carried over services provided by them;
- federal and state and territory laws governing telecommunications interception and access to stored communications, the use of surveillance devices, tracking devices and listening devices, video and audio-visual monitoring of public places and workplaces and computer and data surveillance of workplaces (including home working);
- federal and state/territory freedom of information legislation, applying to information held by government agencies;
- the *Spam Act 2003* (Cth) (**Spam Act**), which deals with the sending of unsolicited commercial electronic messages, including emails and SMS;
- the *Do Not Call Register Act 2006* (Cth)

(**DNCR Act**), regulating unsolicited commercial calling to telephone numbers listed on the national Do Not Call Register (**DNCR**);
- the recently amended *Security of Critical Infrastructure Act 2018* (Cth) which imposes obligations on organisations operating in "critical infrastructure sectors" to ensure the cyber resilience of their assets;
- federal and state criminal laws dealing with unauthorised access to computer systems, including databases; and
- developing judge-made law in the form of an equitable doctrine of misuse of confidential information.

The Privacy Act is administered by the Australian Privacy Commissioner (the **Commissioner**) which is integrated within the Office of the Australian Information Commissioner (**OAIC**). The Australian Communications and Media Authority (**ACMA**) enforces provisions of the Spam Act and the DNCR Act. It also administers a number of privacy affecting codes in the communications sector. The Australian Attorney-General's Department administers provision of lawful assistance to law enforcement agencies under the *Telecommunications (Interception and Access) Act 1979* (Cth), and takes an active role in regulating and enforcing privacy-related legislative schemes.

2. Are there any registration or licensing requirements for entities covered by these laws and, if so, what are the requirements? Are there any exemptions?

There are no registration or licensing requirements under the Privacy Act for general processing of personal information.

3. How do these laws define personal data or personally identifiable information (PII) versus special category or sensitive PII? What other key definitions are set forth in the laws in your jurisdiction?

The following key terms apply under the Privacy Act:

- **Personal Information**

Under the Privacy Act, 'Personal Information' means 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 whether the information or opinion is recorded in a material from or not. State and territory privacy laws use a similar definition.

Whether an individual is 'reasonably identifiable' from particular information will depend on considerations that include:

- the nature and amount of information;
- the circumstances of its receipt;
- who will have access to the information;
- other information either held by or available to the entity that holds the information;
- whether it is possible for the individual or entity that holds the information to identify the individual, using available resources (including other information available to that individual or entity). Where it may be possible to identify an individual using available resources, the practicality, including the time and cost involved, will be relevant to deciding whether an individual is 'reasonably identifiable'; and
- if the information were to be publicly released, whether a reasonable member of the public who accesses that information would be able to identify the individual.

- **APP Entity**

The majority of obligations under the Privacy Act apply to 'APP Entities'. An APP Entity is either a federal government agency (but not a state or territory agency) or any private sector organisation (which includes individuals, companies, partnerships or otherwise) that has an annual turnover greater than AUD3 million which has an Australian link (see below). In addition, an organisation with annual turnover lower than AUD3 million will be an APP Entity if it: (a) provides health services and holds health information; (b) exchanges personal information for a benefit, service or advantage; (c) provides services to a federal government agency (either directly or as a subcontractor); or (d) is a credit reporting body.

- **Sensitive Information**

'Sensitive information' means information or an opinion about an individual's:

- racial or ethnic origin;
- political opinions;
- membership of a political association;
- religious beliefs or affiliations;
- philosophical beliefs;
- membership of a professional or trade association;
- membership of a trade union;

- sexual orientation or practices; or
- criminal record,

that is also personal information; or

- health information about an individual;
- genetic information about an individual that is not otherwise health information;
- biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
- biometric templates.

- **Use and Disclosure**

'Use' and 'disclosure' are key concepts, but are not specifically defined. Guidelines provided by the Privacy Commissioner include the following guidance:

- 'use' — generally, an APP Entity uses personal information when it handles and manages that information within the entity's effective control.
- 'disclosure' — an APP Entity discloses personal information when it makes it accessible or visible to others outside the entity and releases the subsequent handling of the personal information from its effective control.

Importantly, the Privacy Act does not distinguish 'processing' of Personal Information as distinct from other types of 'Use'. Further, the Privacy Act does make a distinction between 'controllers' and 'processors' of personal information.

- **Collects**

An APP Entity collects personal information only if the entity collects the personal information for inclusion in a record or generally available publication.

- **De-identified**

The Privacy Act does not define the term 'de-identified', however, it is an important principle in determining whether or not information is 'Personal Information', that is when it can be said that 'de-identified' information is no longer information about an identifiable individual or an individual who is reasonably identifiable. The Commissioner notes that de-identification includes two steps: firstly removing personal identifiers, such as an individual's name, address, date of birth or other identifying information, and secondly removing or altering other information that may allow an individual to be identified, for example, because of a rare characteristic of the individual, or a combination of unique or remarkable characteristics that enable identification.

De-identification can be effective in preventing re-identification of an individual, but may not remove that risk altogether. There may, for example, be a possibility that another dataset or other information could be matched with the de-identified information. The risk of re-identification must be actively assessed and managed to mitigate this risk. This should occur both before an information asset is de-identified and after disclosure of a de-identified asset.

- **Holds**

A number of APPs (such as APP 6, 11, 12 and 13) apply to an APP Entity that 'holds' personal information.

An entity 'holds' personal information "if the entity has possession or control of a record that contains the personal information". The term 'holds' extends beyond physical possession of a record to include a record that an APP Entity has the right or power to deal with. This means that one entity can physically possess personal information that another entity controls. In such situations, both entities will 'hold' the information at the same time. If each entity is covered by the Privacy Act, each will have separate regulatory obligations to comply with the Privacy Act (since there is no distinction between a controller and a processor).

- **Australian link**

The obligations under the Privacy Act are only applicable to entities if they have an 'Australian link'. The APPs have extra-territorial application and will extend to an act done, or practice engaged in, outside Australia by an organisation, or small business operator, that has an 'Australian link' (s 5B(1A)).

An organisation or small business operator has an Australian link if the organisation or operator is:

- an Australian citizen or a person whose continued presence in Australia is not subject to a legal time limitation;
- a partnership formed, or a trust created, in Australia or an external Territory;
- a body corporate incorporated in Australia or an external Territory; or
- an unincorporated association that has its central management and control in Australia or an external Territory.

An organisation that does not fall within one of those categories will also have an Australian link where both of the following apply:

- it carries on business in Australia or an external Territory; and
- it collected or held personal information in Australia or an external Territory, either before or at the time of the act or practice.

- **Data Subject**

The Privacy Act does not use the term 'Data Subject', but the Privacy Act applies where personal information about any individual is handled (collected, used or disclosed) by a relevant APP Entity. It is not relevant whether that individual resides in Australia or is physically present in Australia or provided the personal information directly to the APP Entity. Conversely, it is the APP Entity's connection to Australia that triggers the application of the Privacy Act, as referred to above.

4. What are the principles related to, the general processing of personal data or PII – for example, must a covered entity establish a legal basis for processing personal data or PII in your jurisdiction or must personal data or PII only be kept for a certain period? Please outline any such principles or "fair information practice principles" in detail.

The following are key Australian Privacy Principles:

- **Transparency**

Under APP 1, APP Entities are required to manage personal information in an open and transparent way and must take reasonable steps to implement practices, procedures and systems to comply with the Privacy Act. This includes an obligation to have a clearly expressed and up to date privacy policy available to the public free of charge and in an appropriate form. Practices and processes must also reflect the stated privacy policy: the Commissioner has also interpreted APP 1 as requiring implementation of 'privacy by design' into an APP Entity's business practices.

APP 5 requires an APP Entity that collects personal information about an individual to take reasonable steps, at or before the time of collection, or as soon as practicable afterwards, either to notify the individual of certain matters or to ensure the individual is aware of those matters. APP 5.2 lists the matters that must be notified to an individual or of which they must be made aware.

The requirement to notify or ensure awareness of the APP 5 matters applies to all personal information collected about an individual, either directly from the individual or from a third party.

- **Lawful basis for processing**

The Privacy Act governs the collection, holding, use, disclosure, access and correction of personal information by APP Entities. The Privacy Act prohibits an organisation from collecting personal information (which is not sensitive information) unless the information is reasonably necessary for one or more of the organisation's functions or activities.

Where an organisation is collecting sensitive information, as with ordinary categories of personal information, it must be reasonably necessary for one or more of the organisation's functions or activities, but it must also obtain the relevant individual's consent to the collection of their sensitive information (unless an exception applies).

The state and territory privacy legislation apply analogous concepts in relation to entities regulated by those Acts.

- **Purpose limitation**

In accordance with APP 6, an APP Entity can only use or disclose personal information for the particular purpose for which it was collected (known as the 'primary purpose'), or for a 'secondary purpose' if an exception applies.

Use or disclosure of personal information for a 'secondary purpose' is permitted under specific exceptions where that secondary use or disclosure is:

- consented to by the individual;
- one in respect of which the individual would reasonably expect the APP Entity to use or disclose their personal information, and that purpose is related to the primary purpose of collection, or, in the case of sensitive information, *directly* related to the primary purpose;
- required or authorised by or under an Australian law or a court or tribunal order;
- necessary to lessen or prevent a serious threat to any individual's life, health or safety, or to public health or safety, and it is unreasonable or impracticable to obtain the consent of the individual;
- necessary in order for an organisation to take appropriate action in relation to a reasonable suspicion of unlawful activity, or misconduct of a serious nature, that relates to the APP Entity's functions or activities. APP 6.2(e) also

permits the use or disclosure of personal information for a secondary purpose to an enforcement body for one or more enforcement related activities;
- in the conduct of surveillance activities, intelligence gathering activities or monitoring activities, by a law enforcement agency;
- the conduct of protective (for example, in relation to children) or custodial activities;
- to assist any APP Entity, body or person to locate a person who has been reported as missing (where the entity reasonably believes that this use or disclosure is reasonably necessary, and where that use or disclosure complies with rules made by the Commissioner);
- for the establishment, exercise or defence of a legal or equitable claim; or
- for the purposes of a confidential alternative dispute resolution process.

- **Data minimisation**

As mentioned above, under APP 3, an organisation must not collect personal information unless the information is reasonably necessary for one or more of the entity's functions or activities. In the case of sensitive information, it must also have the individual's consent.

- **Integrity**

Under APP 10, APP Entities are required to ensure that the personal information they use or disclose is accurate, up-to-date, complete and relevant.

- **Retention**

In accordance with APP 11.2, where an APP Entity holds personal information about an individual which is no longer needed for any purpose for which the information may be used or disclosed, then the APP Entity must take such steps as are reasonable in the circumstances to destroy or de-identify the information.

APPs 4.3 and 11.2 require the destruction or de-identification of personal information in certain circumstances. Where the information is contained in a Commonwealth (Federal) record (which is the property of the Commonwealth), or is required to be retained under Australian law or by a court or tribunal, the information must be retained. For example, financial records must be retained under the *Corporations Act 2001* (Cth) for seven years.

- **Collection by lawful and fair means**

An APP Entity must collect personal information only by "lawful and fair means" (APP 3.5). This requirement applies to all APP Entities. Examples of where a collection of personal information may be unfair (some may also be unlawful) include collecting from an electronic device which is lost or left unattended, collecting from an individual who is traumatised, in a state of shock or intoxicated, collecting in a way that disrespects cultural differences or after misrepresenting the purpose or effect of collection, or the consequences for the individual of not providing the requested information.

- **Collecting directly from the individual**

APP 3.6 provides that an APP Entity "must collect personal information about an individual only from the individual", unless one of the following exceptions applies:

- for all APP Entities, it is unreasonable or impracticable for the entity to collect personal information only from the individual;
- for federal government agencies, the individual consents to the personal information being collected from someone other than the individual; and
- for federal government agencies, the agency is required or authorised by or under an Australian law, or a court or tribunal order, to collect the information from someone other than the individual.

- **Direct marketing**

APP 7 provides that an organisation must not use or disclose personal information it holds for the purpose of direct marketing unless an exception applies. Exceptions include where an individual would reasonably expect an organisation to use or disclose personal information for direct marketing, or where the individual has consented.

Although not specifically defined in the Privacy Act, direct marketing may include the use or disclosure of personal information to communicate directly with an individual to promote goods and services. Examples include displaying an advertisement on a social media site that an individual is logged into, using personal information, including personal data collected by cookies relating to websites the individual has viewed, or sending an email to an individual about a store sale, or other advertising material relating to the store, using personal information provided by the customer in the course of signing up for a store loyalty card.

Where an organisation is permitted to use or disclose personal information for the purpose of direct marketing, it must always: allow an individual to request not to

receive direct marketing communications (also known as 'opting out'), and comply with that request.

- **Cross-border disclosure of personal information**

Before an APP Entity discloses personal information to an overseas recipient, the entity must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information (APP 8.1). This is usually achieved by the APP Entity imposing contractual obligations on the overseas recipient to comply with the Privacy Act (or relevant aspects)

An APP Entity that discloses personal information to an overseas recipient is accountable for any acts or practices of the overseas recipient in relation to the information that would breach the APPs (section 16C).

There are exceptions to the requirement in APP 8.1 to take reasonable steps and to the accountability provision in section 16C. These include obtaining the consent of the relevant individual to the overseas disclosure (after an express statement informing the individual that APP 8 will not apply), or where the APP Entity reasonably believes that the recipient is subject to an equivalent regime in its local jurisdiction and that there are mechanisms that the individual can access to take action to enforce that regime.

- **Security of personal information**

APP 11 requires an APP Entity to take active measures to ensure the security of personal information it holds, and to actively consider whether it is permitted to retain personal information. An APP Entity that holds personal information must take reasonable steps to protect the information from misuse, interference and loss, as well as unauthorised access, modification or disclosure (APP 11.1). Unauthorised access includes both access by an employee of the entity or independent contractor and unauthorised access by an external third party (such as by hacking).

Reasonable steps should include, where relevant, taking steps and implementing strategies in relation to governance, culture and training, internal practices, procedures and systems, ICT security, access security, third party providers (including cloud computing), data breaches, physical security, destruction and de-identification and compliance with applicable standards.

The Commissioner not infrequently determines that internal or external data breaches are reasonably attributable to a failure by an APP Entity to take reasonable steps to protect information security or to take reasonable steps to destroy personal information or ensure it is de-identified if it no longer needs the information for any purpose for which it may be used or disclosed under the APPs.

5. Are there any circumstances where consent is required or typically used in connection with the general processing of personal data or PII?

There is no general requirement to obtain consent for the collection of most types of personal information, or for its processing. However, consent may operate as an exception to certain prohibitions under the Privacy Act or a qualification to certain obligations.

Under APP 3.3, APP Entities are prohibited from collecting sensitive information (defined above) unless the consent of the relevant individual has been obtained. Some narrow exceptions apply.

Under APP 3.6 there is a general expectation that Personal Information will be collected from the individual to which it relates. However, an exception applies which permits government agencies to collect personal information from another source if the individual has given consent.

APP 6 requires Personal Information to only be used or disclosed for the purpose for which it was collected. However, there are some exceptions to this, one being where the individual has consented to its use or disclosure for another secondary purpose.

Under APP 7, direct marketing is prohibited unless an exception applies, and one such exception is where the organisation has obtained the individual's consent. Further, consent is the only permitted circumstance where Sensitive Information can be used for the purpose of direct marketing. The Spam Act also prohibits commercial electronic communications without consent (which may be inferred) and requires entities to allow individuals to easily withdraw consent (or "unsubscribe").

APP 8, which generally restricts the offshore disclosure of Personal Information, allows it to occur where there is consent of the relevant individual (but note this consent has separate requirements under the Privacy Act).

6. What are the rules relating to the form, content and administration of such consent? For instance, can consent be implied, incorporated into a broader

document (such as a terms of service) or bundled with other matters (such as consents for multiple processing operations)?

Where consent is applicable, under the Privacy Act, it may be express or implied. Express consent can be provided orally or in writing, although best practice requires written consent (which can be electronic). Implied consent is consent which can reasonably be inferred from the conduct. The Privacy Commissioner's guidance suggests that consent can only be implied in clear circumstances. For example, it will not be sufficient to merely establish that the collection, use or disclosure will be advantageous to the individual or that they didn't object at the time of collection. The Privacy Commissioner also advises against the use of opt-out mechanisms.

The Privacy Commissioner has identified 4 elements of consent:

- (**informed**) the individual must be adequately informed of the implications of providing or withholding consent for it to be considered informed.
- (**voluntary**) the individual must have a genuine opportunity to provide or withhold consent. This may require an assessment of the alternatives available to the individual if they do not consent and the seriousness of the consequences. Bundling consent may also be problematic for assessing whether consent is voluntary, as the broader consequences of a refusal need to be considered.
- (**current and specific**) consent for collection and proposed uses/disclosures should be typically be obtained at the time personal information is collected. If such consent is being sought later, it should be at the time of the proposed use or disclosure requiring consent. Consent should be as directed as possible, and not a broad consent for various activities.
- (**capacity**) APP Entities need to consider whether the individual has capacity to give consent. Ordinarily, this can be presumed, however, the following factors may indicate that further inquiries are required: age, physical or mental disability, temporary incapacity or limited understanding of English.

One of the reforms currently being considered as part of a broader review of the Privacy Act (see item 40 for further details) is to incorporate these elements into the legislation.

7. What special requirements, if any, are required for processing sensitive PII? Are there any categories of personal data or PII that are prohibited from collection?

There are a number of instances where the APPs impose additional restrictions in respect of sensitive information.

APP 3 requires that an individual's consent is always required for the collection of sensitive information under the Privacy Act (unless an exception applies). This differs from other types of personal information where consent is not strictly required.

APP 6 addresses the purpose for which information may be used or disclosed. It provides that where consent has not been obtained, sensitive information can only be used for a secondary purpose if that secondary purpose is *directly* related to the primary purpose (that is, the purpose for which it was collected). This contrasts with other personal information which can be used for any secondary purpose which is related to the primary purpose. The term "directly related" is not expressly defined, however, it is likely to require a secondary purpose which is closely related to the primary purpose.

Under APP 7, the only circumstance in which sensitive information can only be used for the purpose of direct marketing is if the individual has consented. This is narrower than the circumstances for which other types of personal information can be used in this way (for example, where the individual would reasonably expect the information to use the non-sensitive personal information for that purpose and provides a simple means to request that the entity cease marketing).

There are no categories of personal information that are *prohibited* from being collected under the Privacy Act.

8. How do the laws in your jurisdiction address children's personal data or PII?

The Privacy Act itself does not contain additional or special obligations relating to the use or disclosure of children's personal information.

That said, the provisions relating to consent are likely to require an assessment of the relevant capacity of the individual, and guardian consent to be obtained where necessary. The Privacy Commissioner has provided guidance that where an individual is under the age of 18, an assessment of their capacity is required. If it is not practical to assess the capacity of an individual, the Privacy Commissioner has said that, as a general rule, APP Entities should assume that an individual over the

age of 15 has capacity, unless there is evidence to the contrary.

9. Does the law include any derogations, exclusions or limitations other than those already described? Please describe the relevant provisions.

- **Small Business Operators**

As described above, an organisation will not be subject to the obligations under the Privacy Act if its annual turnover is less than AUD3 million. This exception does not apply where the organisation:

- provides health services and holds any health information;
- exchanges personal information for a benefit, service or advantage;
- is a contracted service provider to a federal government agency (whether directly or under a sub-contract); or
- is a credit reporting body.

- **Australian Link**

The obligations under the Privacy Act are only applicable to entities if they have an 'Australian link'. This requirement is described in further detail in the answer to item 3 above.

- **Employee Records**

Acts or practices of an organisation which is a private sector employer of an individual which are directly related to: (i) a current or former employment relationship between the organisation and the individual; and (ii) records of personal information relating to the individual's employment, are exempt from the obligations of the Privacy Act. Note this exemption does not apply to contractors or unsuccessful job applicants.

- **Journalism**

APP Entities engaged in journalism are exempt from the Privacy Act provided they observe alternative standards which address privacy and have been published by an organisation representing a class of media organisations.

- **State Governments and their service providers**

State Governments have adopted their own privacy legislation and are not subject to the Privacy Act. Also, acts undertaken by (sub)contractors to state governments pursuant to such service contracts are exempt from the Privacy Act (however, it will likely be subject to the relevant State legislation).

- **Political parties**

Generally speaking, political parties are exempt from the obligations in the Privacy Act.

- **Individuals in a non-business capacity**

An individual who may constitute an APP Entity because of their business affairs (such as a sole trader) will not be subject to Privacy Act obligations in respect of their personal affairs.

10. Does your jurisdiction impose requirements of 'data protection by design' or 'data protection by default' or similar? If so, please describe the requirement and how businesses typically meet the requirement.

This is not an express requirement of the Privacy Act; however, APP 1 requires APP Entities to take reasonable steps to implement practices, procedures and systems to ensure compliance with the APPs and enable the entity to deal with enquiries or complaints about privacy. The Privacy Commissioner considers that this amounts to a requirement of privacy by design.

Some of the measures the Privacy Commissioner recommends entities take to address this requirement include:

- procedures for identifying and managing privacy risks at each stage of data processing, including collection, use, disclosure, storage, destruction and de-identification;
- security systems for protecting personal information from misuse, interference, loss and unauthorised access, modification or disclosure;
- a commitment to conduct privacy impact assessments in respect of new projects;
- procedures for identifying and responding to privacy breaches, access and correction requests and receiving and responding to complaints or inquiries;
- aiming to give individuals the option to remain anonymous or use a pseudonym when dealing with the organisation;
- governance mechanisms to ensure compliance with the Privacy Act;
- regular staff training;
- appropriate supervision of staff whom regularly handle personal information;

- appropriate mechanisms to ensure that agents and contractors handle personal information consistently with law and the organisations practices and procedures; and
- a program of proactive review and audit of privacy processes and systems.

As mentioned, the obligation under APP 1 is limited to reasonable steps. What is reasonable will depend on the circumstances, in particular the nature of the possible information to be processed, the adverse consequences to individuals of improper use, the nature of the organisation handling the information and the cost and practicality of the steps being considered.

11. Are owners or processors of personal data or PII required to maintain any internal records of their data processing activities or to establish internal processes or written documentation? If so, please describe how businesses typically meet these requirements.

APP 1 expressly requires entities to maintain an up-to-date privacy policy which documents the personal information they collect and how they use and disclose it. Beyond this, there are no express record keeping obligations. However, the broader requirements of APP 1 with respect to the implementation of practices, procedures and systems to ensure compliance with the APPs may necessitate internal compliance policies and processes, including to understand what data is collected, where it is stored, how long it is to be retained, who can access it and what risks it is exposed to. This is often managed by establishing internal privacy and data use and retention policies, requirements for privacy or data impact assessments and data mapping and classification exercises, including with assistance from cyber security teams.

12. Do the laws in your jurisdiction require or recommend having defined data retention and data disposal policies and procedures? If so, please describe these data retention and disposal requirements.

There are no prescriptive requirements in this regard. Under APP 11.2, APP Entities which hold Personal Information which is no longer needed and is not required by law to be retained must take such steps as are reasonable to destroy it or ensure it is de-identified. There are no express timeframes specified for disposal.

The obligation under APP 11.2 is limited to the taking of reasonable steps. What is reasonable will depend on the circumstances, and the following factors may be relevant:

a. the amount and sensitivity of the information;
b. the nature of the organisation;
c. the possible adverse consequences to individuals if the information is mis-handled;
d. the organisation's information handling practices (such as where handling is outsourced); and
e. the time and cost involved in complying.

Certain types of information, such as Tax File Numbers and some health information, have further retention and deletion requirements.

13. When are you required to, or when is it recommended that you, consult with data privacy regulators in your jurisdiction?

The Privacy Commissioner typically acts in response to complaints from individuals or self-reporting from organisations, including under the mandatory data breach notification regime. There is not a formal process for pre-screening or consultation with the Privacy Commissioner the way there may be in other jurisdictions or with other regulators in Australia.

The situation is similar for Federal agencies, although they may be required to provide their privacy impact assessments to the Privacy Commissioner.

14. Do the laws in your jurisdiction require or recommend conducting risk assessments regarding data processing activities and, if so, in what circumstances? How are these risk assessments typically carried out?

Only Federal Government Agencies are subject to an express obligation under the Privacy (Australian Government Agencies – Governance) APP Code 2017 (**Agency Code**) to undertake privacy impact assessments. They must do this for all 'high privacy risk projects'. A project may be a high privacy risk project if the agency reasonably considers that the project involves new or changed ways of handling personal information that are likely to have a significant impact on the privacy of individuals. Agencies are also required to carry out privacy impact assessments where they are directed to do so by the Privacy Commissioner under section 33D of the Privacy Act.

Private sector organisations do not have an express obligation to conduct a privacy impact assessment, however, many choose to in order to address the obligation under APP 1 to take reasonable steps to implement practices, procedures and systems to ensure compliance with the APPs. Completion of a privacy impact assessment can be used to establish that such reasonable steps have been taken, as well as identify other measures to be implemented.

The Privacy Commissioner sets out a 10 step process for conducting a privacy impact assessment. These steps are:

a. conduct a threshold assessment;
b. plan the PIA;
c. describe the project;
d. identify and consult with stakeholders;
e. map information flows;
f. prepare a privacy impact analysis and compliance check;
g. privacy management — addressing risks;
h. consider and prepare recommendations;
i. produce a report; and
j. respond and review.

15. Do the laws in your jurisdiction require appointment of a data protection officer (or other person to be in charge of privacy or data protection at the organization) and what are their legal responsibilities?

Only Government agencies are required to have a privacy officer. This is pursuant to the Agency Code applicable to them. Other larger organisations sometimes appoint a privacy officer despite not having a strict obligation to do so.

The Privacy Officer functions required under the Agency Code include:

a. providing privacy advice internally such as:
    i. the development of new initiatives that have a potential privacy impact;
    ii. the general application of privacy law to the agency's activities;
    iii. what to consider when deciding whether or not to carry out a Privacy Impact Assessment; and
    iv. what safeguards to apply to mitigate any risks to the privacy of individuals;
b. liaising with the OAIC;
c. co-ordinating the handling of internal and external privacy enquiries, privacy complaints, and requests for access to, and correction of, personal information;
d. maintaining a record of your agency's personal information holdings;
e. assisting with the preparation of Privacy Impact Assessments; and
f. measuring and documenting your agency's performance against its privacy management plan.

16. Do the laws in your jurisdiction require or recommend employee training? If so, please describe these training requirements.

There are no express requirements, although many choose to in order to address the obligation under APP 1 to take reasonable steps to implement practices, procedures and systems to ensure compliance with the APPs. The Privacy Commissioner provides a number of training resources on its website.

Further, many regulators consider training in respect of cyber security part of general risk management obligation under various laws.

17. Do the laws in your jurisdiction require businesses to providing notice to individuals of their processing activities? If so, please describe these notice requirements (e.g., posting an online privacy notice).

APP 1 requires organisations to have a Privacy Policy setting out the types of information the organisation collects, and how it is used or disclosed. Privacy policies are required to be clearly expressed and made available free of charge. Organisations typically publish their privacy policies on their public-facing website.

A privacy policy must contain:

- the kinds of information that the entity collects and holds;
- how it collects and holds information;
- the purposes for which the entity collects, holds, uses and discloses information;
- how an individual may access their information and seek correction;
- how an individual can make a complaint, and how the organisation will deal with the complaint; and
- whether the organisation will disclose the

personal information to an overseas recipient, and if so the countries in which such recipients are likely to be located.

Further, APP 5 requires organisations to take reasonable steps to provide a collection notice to individuals at or before the time they are collecting personal information (or as soon as practicable after). This notice must include:

- the identity and contact details of the organisation;
- the fact that information is being collected (this is particularly important where the collection is from a third party or the collection is not obvious);
- where the collection is required by law, that fact and the details of the law requiring collection;
- the purpose for which the information is being collected;
- the main consequences for the individual if the information is not collected;
- any other entities to which the information will be provided;
- references to the organisation's privacy policy (including a hyperlink if possible); and
- whether the organisation will disclose the personal information to an overseas recipient, and if so the countries in which such recipients are likely to be located.

The obligation under APP 5 is one of reasonable steps only. What is reasonable will depend on the circumstances.

18. Do the laws in your jurisdiction draw any distinction between the owners/controllers and the processors of personal data and, if so, what are they? (e.g., are obligations placed on processors by operation of law, or do they typically only apply through flow-down contractual requirements from the owners/controller?)

Organisations and government agencies that collect, use or disclose personal information are regulated in relation to those activities. Terms such as 'Controller', 'Owner' and 'Processor' are not used in the Privacy Act or state and territory privacy acts. Organisations and federal government agencies that collect, use or disclose personal information are called 'APP Entities' and must comply with the Privacy Act and the APPs contained in the Privacy Act.

In practice, an important and difficult distinction is between APP Entities that collect, use or disclose personal information and organisations that as service providers to those APP Entities may handle personal information for those entities: for example, operations of data warehouses or data centres and cloud as-a-service providers.

Where personal information is entrusted by an APP Entity that collects that personal information to another party for storage and processing, the Commissioner looks to whether the second party has 'control' of that information. If the second party can fully access and edit that information, the provision of that personal information to the second party is a 'disclosure' subject to relevant notice and consent requirements and the second party is an entity that 'collects' this information. However, the Commissioner has expressed the view that in limited circumstances, an APP Entity might retain such a degree of control over the information that the APP Entity is considered to be 'using' that information and not disclosing the information to the second party. For example, where an APP Entity provides personal information to a cloud service provider located overseas, this may be a 'use' if the information is provided for the limited purpose of performing the services of storing and ensuring the APP Entity may access the personal information, and a binding contract between the parties:

- requires the provider only to handle the personal information for these limited purposes;
- requires any subcontractors to agree to the same obligations; and
- gives the entity effective control of how the personal information is handled by the provider. Issues to consider include whether the entity retains the right or power to access, change or retrieve the personal information, who else will be able to access the personal information and for what purposes, what type of security measures will be used for the storage and management of the personal information and whether the personal information can be retrieved or permanently deleted by the entity when no longer required or at the end of the contract.

Whether or not other examples are considered a 'use' or a 'disclosure' will depend on the circumstances of each individual case, having regard to the degree of control held by the APP Entity.

19. Do the laws in your jurisdiction require

minimum contract terms with processors of personal data or PII or are there any other restrictions relating to the appointment of processors (e.g., due diligence or privacy and security assessments)?

No, this is not prescribed. For instance, there is no equivalent to the model clauses required under the EU General Data Protection Regulation 2016/679.

That said, APP Entities may be held liable for the acts and omissions of third party suppliers of services which involve the use, storage or disclosure of personal information collected by the APP Entity. Accordingly, it is common for contracts with such suppliers to include detailed privacy provisions obliging the supplier to comply with the Privacy Act as if it were subject to it and imposing other limitations and restrictions on the supplier in relation to their use and disclosure of the personal information.

In addition, under APP8.1, where an entity discloses personal information to an overseas recipient, the entity disclosing the information must take reasonable steps to ensure that the overseas recipient does not breach the APPs. One typical step taken is to put in place an appropriate contractual regime with the overseas recipient of information.

20. Please describe any restrictions on monitoring, automated decision-making or profiling in your jurisdiction including the use of tracking technologies such as cookies. How are these terms defined and what restrictions are imposed, if any?

These issues are not specifically addressed under Australian law.

However, to the extent that the use of cookies involves the collection, use or disclosure or transfer of personal information, the APPs will apply. The concept of 'collection' of personal information applies broadly, and includes information associated with web browsing, such as personal information collected by cookies. Consequently, collection of personal information using cookies can occur provided that the notice and consent requirements are followed.

21. Please describe any restrictions on cross-contextual behavioral advertising. How is this term or related terms defined?

This is not specifically addressed under Australian law. However, similar to the above comment in item 20 above, to the extent this involves use of personal information (including via cookies) the APPs will apply and need to be complied with.

22. Please describe any laws in your jurisdiction addressing the sale of personal information. How is "sale" or related terms defined and what restrictions are imposed, if any?

There are no provisions in the Privacy Act expressly controlling or prohibiting the sale or other trading of Personal Information. That said, any such sale must comply with the APPs and other obligations under the Privacy Act. For example, a sale would constitute a disclosure of Personal Information, so the requirements of APP 6 must be met.

Further, an organisation will be an APP entity (i.e., subject to the requirements of the Privacy Act) if it is in the business of selling personal information. This is so even if the organisation would otherwise be exempt as a small business.

23. Please describe any laws in your jurisdiction addressing telephone calls, text messaging, email communication or direct marketing. How are these terms defined and what restrictions are imposed, if any?

Electronic marketing is partly regulated through subject matter-specific federal laws such as the Spam Act, which governs most forms of electronic marketing, and the DNCR Act, which regulates unsolicited telemarketing calls.

APP 7 of the Privacy Act also regulates use or disclosure of personal information for the purpose of direct marketing activities.

Generally, organisations may only use or disclose personal information for direct marketing purposes where the individual has either consented (expressly or impliedly) to their personal information being used for direct marketing, or has a reasonable expectation that their personal information will be used for this purpose, and conditions relating to provision by the organisation of an opt-out mechanism are met.

The Spam Act prohibits 'unsolicited commercial electronic messages' with an 'Australian link' from being

sent or caused to be sent. Commercial electronic messages may only be sent with an individual's consent (express or inferred in certain circumstances), and the message contains accurate sender identification and a functional unsubscribe facility. The burden of proving consent lies with the sender of the message.

Voice calls, including synthetic or recorded calls (such as robocalls), are separately regulated under a 'do not call' regulatory framework established under the DNCR Act and associated legislation and instruments, including the *Telecommunications Act 1997* (Cth) (**Telecommunications Act**), under which individuals may complain about potential breaches of the Spam Act and the DNCR Act, and the Telecommunications (Do Not Call Register) (Telemarketing and Research Calls) Industry Standard 2007. Marketing faxes are also regulated. A telemarketing call or marketing fax is broadly defined as a voice call or fax made to a number to offer, supply, provide, advertise or solicit goods or services, land or an interest in land, a business/investment opportunity and donations. Certain calls are not considered to be telemarketing or fax marketing, including product recall, fault verification, appointment rescheduling, appointment reminder, payments and solicited calls/faxes about orders, requests or customer enquiries.

The DNCR Act provides an 'opt-out' option, allowing Australians who do not wish to receive telemarketing calls or marketing faxes to list their private-use fixed and mobile telephone numbers and fax numbers on the DNCR. As of June 2021, total DNCR registrations exceed 10.35 million. The quantity of numbers that telemarketers and fax marketers submit for checking (or 'washing') against the DNCR was 620 million during the 2020-21 financial year.

Unsolicited telemarketing calls or faxes must not be made to an Australian number registered on the DNCR without the consent (implied or express) of the relevant account holder or their nominee.

24. Please describe any laws in your jurisdiction addressing biometrics, such as facial recognition. How are these terms defined and what restrictions are imposed, if any?

The definition of 'sensitive information' includes: (i) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; and (ii) biometric templates, so the obligations applicable to sensitive information will apply. These are set out in the answer to item 7 above. Besides this, there are no specific requirements under the Privacy Act.

25. Is the transfer of personal data or PII outside the jurisdiction restricted? If so, please describe these restrictions and how businesses typically comply with them (e.g., does a cross-border transfer of personal data require a specified mechanism? Does a cross-border transfer of personal data or PII require notification to or authorization from a regulator?)

Before an APP Entity discloses personal information to an overseas recipient, the entity must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information (APP 8.1). Reasonable steps typically requires that the APP Entity enter into an enforceable contract with the overseas recipient which includes obligations consistent with the APPs. Alternatively, disclosure is also permissible where the APP Entity reasonably believes that the overseas entity is subject to laws or a binding scheme which is at least substantially similar to the APPs and the individual has mechanisms available to them to enforce that protection.

An APP Entity that discloses personal information to an overseas recipient is generally accountable for any acts or practices of the overseas recipient in relation to the information that would breach the APPs (section 16C).

However, there are exceptions to the requirement in APP 8.1 to take reasonable steps and to the accountability provision in section 16C. These include obtaining the consent of the relevant individual to the overseas disclosure (after an express statement informing the individual that APP 8 will not apply), or where the APP Entity reasonably believes that the recipient is subject to an equivalent regime in its local jurisdiction and that there are mechanisms that the individual can access to take action to enforce that regime.

26. What security obligations are imposed on personal data or PII owners/controllers and on processors, if any, in your jurisdiction?

APP 11 requires an APP Entity to take active measures to ensure the security of personal information it holds, and to actively consider whether it is permitted to retain personal information. An APP Entity that holds personal information must take reasonable steps to protect the

information from misuse, interference and loss, as well as unauthorised access, modification or disclosure (APP 11.1). Unauthorised access includes both access by an employee of the entity or independent contractor and unauthorised access by an external third party (such as by hacking).

Reasonable steps should include, where relevant, taking steps and implementing strategies in relation to governance, culture and training, internal practices, procedures and systems, ICT security, access security, third party providers (including cloud computing), data breaches, physical security, destruction and de-identification and compliance with applicable standards.

The Commissioner not infrequently determined that internal or external data breaches are reasonably attributable to a failure by an APP Entity to take reasonable steps to protect information security or to take reasonable steps to destroy personal information or ensure it is de-identified if it no longer needs the information for any purpose for which it may be used or disclosed under the APPs.

In addition, certain types of information (such as tax file numbers) and certain sectors (such as the financial services sector) are subject to additional cyber security requirements, including under Prudential Standard CPS 234 and the SOCI Act, as referred to below, and also via general risk management obligations, including under section 912A of the *Corporations Act 2001* (Cth).

27. Do the laws in your jurisdiction address security breaches and, if so, how does the law define "security breach"?

Part IIIC of the Privacy Act sets out a regime for the notification of 'Eligible Data Breaches'. The specifics of the regime are set out in the answer to item 29.

An Eligible Data Breach occurs where:

a. there is unauthorised access to, or unauthorised disclosure of personal information or personal information is lost in circumstances where unauthorised access to, or unauthorised disclosure of the information is likely to occur; and
b. a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates.

The potential harm contemplated in this definition includes physical, psychological, emotional, economic and financial harm, as well as harm to reputation. An assessment as to whether an individual is likely to suffer 'serious harm' as a result of an Eligible Data Breach depends on, among any other relevant matters:

- the kind and sensitivity of the information subject to the breach;
- whether the information is protected and the likelihood of overcoming that protection;
- if a security technology or methodology is used in relation to the information to make it unintelligible or meaningless to persons not authorised to obtain it – the information or knowledge required to circumvent the security technology or methodology;
- the persons, or the kinds of persons, who have obtained, or could obtain, the information; and

the nature of the harm that may result from the data breach.

28. Does your jurisdiction impose specific security requirements on certain sectors, industries or technologies (e.g., telecoms, infrastructure, artificial intelligence)?

The *Security of Critical Infrastructure Act 2018* (Cth) (**SOCI Act**) was amended in 2021 and again in 2022 to ensure the strengthened resiliency of and protection of Australian businesses in critical sectors from sophisticated cyber threats. The SOCI Act imposes obligations on businesses in the following sectors which are considered 'critical infrastructure sectors':

- the communications sector;
- the financial services and markets sector;
- the data storage or processing sector;
- the defence industry sector;
- the higher education and research sector;
- the energy sector;
- the food and grocery sector;
- the health care and medical sector;
- the space technology sector;
- the transport sector; and
- the water and sewerage sector.

Certain businesses in these sectors may be required to (among other things):

- provide information regarding the assets it uses in the conduct of its business (including regarding the ownership and operation of those assets) for inclusion in the federal government's register of critical infrastructure assets;

- adopt and maintain an all-hazards critical infrastructure risk management program to address, among other things, cyber risks;
- notify the Australian Signals Directorate of cyber incidents affecting an entity's critical infrastructure assets, with (verbal) notification required within 12 hours if the cyber incident is likely to have a significant impact on the availability of the asset; and
- where assets are declared to be systems of national significance, comply with additional security obligations, including development of a cyber incident response plan, conduct of cyber security rehearsal exercises, and vulnerability assessments.

In addition, the SOCI Act provides the federal government with various access and intervention powers to address security vulnerabilities in critical assets and managing response to cyber incidents.

Entities that fail to comply with obligations under the SOCI Act are liable for fines, with maximum penalties ranging up to AUD277,500. The SOCI Act also includes criminal offences.

Outside of the SOCI Act, regulated entities in the financial services sector (for example, banks, insurers and superannuation providers) must comply with cyber security standards as part of their prudential regulation. Prudential Standard CPS 234 aims to bolster the cybersecurity readiness of regulated entities and minimising the likelihood and impact of incidents on confidentiality, integrity or availability of information and information systems.

CPS 234 places obligations on these regulated financial services entities with respect to how they manage their 'information assets'. Information assets are defined to mean both data and the IT systems used to operate the business. These obligations cover cyber risk management, implementation of security controls, testing and audit of those security controls and cyber incident response.

If a cyber incident occurs which has the potential to materially affect (whether financially or otherwise) the interests of depositors, policyholders, beneficiaries or customers, then the entity is required to notify the Australian Prudential Regulation Authority (**APRA**) within 72 hours. Entities must also notify APRA of any incidents which it has had to notify to another regulator (for example an Eligible Data Breach notification to the Privacy Commissioner under the Privacy Act).

The Telecommunications sector is another which has specific cybersecurity requirements. The telecommunication sector security reforms (**TSSR**) were introduced in 2017 as amendments to the *Telecommunications Act 1997* (Cth) to establish a regulatory framework to better manage the national security risks of espionage, sabotage and foreign interference to Australia's telecommunications networks and facilities. The TSSR contain the following key elements:

- Security obligation: all carriers, carriage service providers and carriage service intermediaries will be required to do their best to protect networks and facilities from unauthorised access and interference – including a requirement to maintain 'competent supervision' and 'effective control' over telecommunications networks and facilities owned or operated by them.
- Notification obligation: carriers and nominated carriage service providers will be required to notify government of planned changes to their systems and services that could compromise their capacity to comply with the security obligation.
- Information gathering power: the Secretary of the Department of Home Affairs has the power to obtain information and documents from carriers, carriage service providers and carriage service intermediaries, to monitor and investigate their compliance with the security obligation.

Directions power: the Home Affairs Minister has a new directions power, to direct a carrier, carriage service provider or carriage service intermediary to do, or not do, a specified thing that is reasonably necessary to protect networks and facilities from national security risks.

29. Under what circumstances must a business report security breaches to regulators, to individuals, or to other persons or entities? If breach notification is not required by law, is it recommended by the regulator and what is the typical custom or practice in your jurisdiction?

Where an APP Entity is aware that there are reasonable grounds to believe that there has been an Eligible Data Breach (whether it forms such an awareness following an assessment of a reasonable suspicion that an Eligible Data Breach may have occurred (which such assessment must take no more than 30 days), or otherwise), the entity must *as soon as practicable*:

a. prepare a statement that, at a minimum, contains:
    i. the entity's contact details. If relevant, the identity and contact details of any entity that jointly or simultaneously holds the same information in respect of which the eligible data breach has occurred, for example, due to outsourcing, joint venture or shared services arrangements may also be provided. If this information is included in the statement, that other entity will not need to separately report the eligible data breach;
    ii. a description of the data breach;
    iii. the kinds of information concerned; and
    iv. the steps it recommends individuals take to mitigate the harm that may arise from the breach. (While the entity is expected to make reasonable efforts to identify and include recommendations, it is not expected to identify every possible recommendation that could be made following a breach);
b. provide a copy of this statement to the OAIC; and
c. take such steps as are reasonable in the circumstances to notify affected or at risk individuals of the contents of the statement. Individuals may be notified by the mode of communication normally used by the entity, or if there is no normal mode of communication, by email, telephone or post. If direct notification is not practicable, the entity must publish the statement on its website and take reasonable steps to publicise its contents.

The OAIC provides a standard form which may be used to notify, found here.

What constitutes a 'practicable' timeframe will vary depending on the time, effort or cost required to comply with the above requirements.

Additional reporting requirements may apply based on the sector as described in item 28 above, including under both the SOCI Act and CPS 234.

30. Does your jurisdiction have any specific legal requirement or guidance regarding dealing with cyber-crime, such as the payment of ransoms in ransomware attacks?

The stated policy of the Australian Government is that ransoms should never be paid, however, payment of ransoms is not expressly outlawed, subject to compliance with sanctions law and laws relating to funding of criminal or terrorist organisations.

As described above, there are a number of sector specific laws which require reporting of cyber incidents. This includes the SOCI Act, which requires certain incidents to be notified within 12 hours.

There are current reforms being contemplated which would require organisations to report all cyber incidents and ransom payments to the Department of Home Affairs.

31. Does your jurisdiction have a separate cybersecurity regulator? If so, please provide details.

As Australian law dealing with cybersecurity is still piecemeal, there are a number of regulators with responsibilities. Some such regulators are set out below.

- The Privacy Commissioner which has responsibility for security related aspects of privacy law.
- The Department of Home Affairs which administers the SOCI Act.
- A number of industry specific regulators in sectors for which there are cyber specific obligations (for example, APRA in respect of financial services).

The Australian Cyber Security Centre (ASCS) which is part of the Australian Signals Directorate and is tasked with leading the federal government's operational response to cyber issues, but which has minimal regulatory powers at present.

32. Do the laws in your jurisdiction provide individual data privacy rights, such as the right to access and the right to deletion? If so, please provide a general description of the rights, how they are exercised, what exceptions exist and any other relevant

details.

- **Access to data**

An APP Entity that holds personal information about an individual must, on request, give that individual access to the information (APP 12.1).

APP 12 also sets out minimum access requirements, including the time period for responding to an access request, how access is to be given, and that a written notice, including the reasons for the refusal, must be given to the individual if access is refused. For example, an APP Entity must respond to a request for access to the personal information if the entity is an agency, within 30 days after the request is made, or if the entity is an organisation, within a reasonable period after the request is made.

There are a number of exceptions to the obligation for organisations to provide an individual access to their personal information, including where the entity reasonably believes that:

- giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or
- giving access would have an unreasonable impact on the privacy of other individuals.

- **Correction and deletion**

APP 13.1 provides that an APP Entity must take reasonable steps to correct personal information it holds, to ensure it is accurate, up-to-date, complete, relevant and not misleading, having regard to the purpose for which it is held.

APP 13.1 requires an APP Entity to take reasonable steps to correct personal information it holds, in two circumstances: on its own initiative, and at the request of the individual to whom the personal information relates.

Upon receiving a request an entity must decide if it is satisfied that the information is incorrect, and if so, take reasonable steps to correct it.

APP 13 does not stipulate formal requirements that an individual must follow to make a request, require that a request be made in writing, or require the individual to state that the request is an APP 13 request.

- **Objection to processing**

There is no general right for an individual to object to collection, use or disclosure of personal information. The Privacy Act generally only requires notice of processing activities to be provided to individuals, and consent is only required in relation to particular activities, notably including collection, use or disclosure of sensitive information and use and disclosure of personal information for the purpose of direct marketing.

However, APP 2 provides that individuals must have the option of dealing anonymously or by pseudonym with an APP Entity. However, an APP Entity is not required to provide those options where:

- the entity is required or authorised by law or a court or tribunal order to deal with identified individuals; or
- it is impracticable for the entity to deal with individuals who have not identified themselves (which is often the case).

Anonymity means that an individual dealing with an APP Entity cannot be identified and the entity does not collect personal information or identifiers.

A pseudonym is a name, term or descriptor that is different to an individual's actual name.

Where applicable, an APP Entity must ensure that individuals are made aware of their opportunity to deal anonymously or by pseudonym with the entity.

- **Complaint to relevant data protection authority(ies)**

An individual has the right to lodge a complaint with the Privacy Commissioner for alleged breaches of the Privacy Act. Generally, the complainant must first register a complaint with the APP Entity to which the complaint relates. If dissatisfied with the response, a complainant can complain to the Commissioner or to an external dispute resolution scheme of which the entity is a member (if applicable). In conducting its investigations, the Commissioner may require the production of documents and information, and compel people to appear and answer questions.

33. Are individual data privacy rights exercisable through the judicial system or enforced by a regulator or both?

Individual data privacy rights are only exercisable through the regulator, which is the Privacy Commissioner. Affected individuals can lodge complaints with the Privacy Commissioner which has a formal investigation and conciliation, or determination process prescribed in the Privacy Act.

34. Does the law in your jurisdiction provide for a private right of action and, if so, in what circumstances?

The Privacy Act does not currently provide a private right to claim damages, only a right to enforce a declaration by the Privacy Commissioner for compensation or to seek an injunction. The private right to seek injunctive relief has been used very infrequently.

There are current proposals for law reform being considered at the moment which would introduce a private right of action and/or a statutory tort for invasion of privacy which could be enforced by individuals. These reforms are discussed further in item 40.

We note that privacy breaches may arise in circumstances which also constitute a breach of confidentiality. Where this is the case, individuals may have rights under a contract with the entity or an equitable duty of confidentiality may also apply.

35. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data privacy laws? Is actual damage required or is injury of feelings sufficient?

The Privacy Commissioner has power to award compensation to individuals affected by breaches of the Privacy Act. This is available both for financial loss as well as for non-economic losses, such as emotional harm, humiliation or inconvenience.

The Privacy Commissioner has applied the following principles in awarding compensation:

a. principles of damages applied in tort law will assist in measuring compensation;
b. compensation should be assessed having regard to the complainant's reaction (not a 'reasonable person' test);
c. there must be a good reason not to award compensation once loss is established; and
d. aggravated damages may be awarded in appropriate cases. While aggravated damages are seldom awarded, it is open to the Privacy Commissioner to do so, particularly if:
e. an entity's conduct is considered to be 'high-handed, malicious, insulting or oppressive'; or
f. the entity has acted in a way that exacerbates the complainant's injury or hurt feelings.

36. How are the laws governing privacy and data protection enforced?

The Privacy Commissioner has a range of regulatory powers including powers to:

- conduct an assessment of whether an entity is maintaining and handling personal information in accordance with relevant provisions (such as the APPs);
- direct a government agency (but not private sector organisations) to give the Privacy Commissioner a privacy impact assessment;
- request entities to develop an APP code or impose one where appropriate;
- investigate an entity following a complaint;
- investigate an entity on its own initiative, that is, without someone making a complaint (Commissioner initiated investigation);
- accept an enforceable undertaking from an entity. An enforceable undertaking is a promise by an entity that it will take specified action or refrain from taking specified action in order to comply with relevant privacy provisions, or to ensure it does not do an act or engage in a practice that interferes with an individual's privacy;
- make a determination on a privacy complaint. The Privacy Commissioner can also make a determination after conducting a Commissioner initiated investigation; and
- apply to the courts for an injunction to restrain a person from engaging in conduct that would constitute a breach of relevant privacy provisions or for an order that an entity pay the civil penalty.

The Privacy Act provides several complaints paths for individuals where there has been (or is suspected to have been) a breach of an APP. The primary complaints process is through a complaint to the Privacy Commissioner, initiating an investigation by the Privacy Commissioner (sections 36 and 40). This process typically requires that the individual has first complained to the relevant APP Entity.

An investigation may result in a determination by the Privacy Commissioner, containing a declaration that:

- the respondent's conduct constituted an interference with the privacy of an individual and must not be repeated or continued;
- the respondent must take specified steps within a specified period to ensure that such conduct is not repeated or continued;
- the respondent must perform any reasonable

act or course of conduct to redress any loss or damage suffered by the complainant;
- the complainant is entitled to a specified amount by way of compensation for any loss or damage suffered by reason of the act or practice the subject of the complaint; or
- that no further action is needed (section 52(1)).

A complainant may apply to the Federal Court of Australia or the Federal Circuit Court of Australia to enforce a determination of the Commissioner (section 55A). An individual may also apply to the Federal Court or Federal Circuit Court for an injunction where a person has, is, or is proposing to engage in conduct that was or would be a breach of the Privacy Act (section 98).

There is not a private right to claim damages, only a right to enforce a declaration by the Privacy Commissioner for compensation or to seek an injunction. The private right to seek injunctive relief has been used very infrequently.

Section 80W of the Privacy Act empowers the Privacy Commissioner to apply to the Federal Court or Federal Circuit Court for an order that an entity, that is alleged to have contravened a civil penalty provision, pay a civil penalty. A civil penalty order financially penalises an entity, but does not compensate individuals adversely affected by the contravention.

The 'civil penalty provisions' in the Privacy Act include:

- a serious or repeated interference with privacy (s 13G) – 2000 penalty units, and
- various civil penalty provisions set out in Part IIIA – which are only applicable to credit reporting bodies and credit providers – penalties of either 500, 1000 or 2000 penalty units.

The current maximum civil penalty that may be imposed is AUD2.22 million for corporate entities. It is important to note that while other enforcement actions (such as the making of determinations and the award of compensation) can be made by the Privacy Commissioner, liability for civil penalties only arises where it is ordered by the Federal Court.

Where an APP Entity experiences an Eligible Data Breach, the occurrence of that data breach in and of itself is unlikely to result in the entity facing penalties. However, a failure to (amongst other things):

- if an entity has a reasonable suspicion that there may have been an eligible data breach, carry out a reasonable and expeditious assessment of whether there are reasonable grounds to believe that an eligible data breach occurred and to take all reasonable steps to ensure that that assessment is completed within 30 days after the entity becomes suspicious; and
- report an eligible data breach,

will be considered an "*interference with the privacy of an individual*" affected by the Eligible Data Breach (section 13(4A)).

37. What is the range of sanctions (including fines and penalties) for violation of these laws?

As mentioned above, civil penalties may be imposed for a serious or repeated interference with privacy. The current maximum civil penalty that may be imposed is AUD2.22 million for corporate entities.

There are also a number of civil penalty provisions which are applicable to credit reporting bodies and credit providers who use or disclose information in contravention of the Privacy Act. The current maximum civil penalty that may be imposed is AUD2.22 million for corporate entities.

38. Are there any guidelines or rules published regarding the calculation of fines or thresholds for the imposition of sanctions?

No, civil penalties are a matter for Court discretion and there are no guidelines in the Privacy Act (other than the maximum penalty).

39. Can personal data or PII owners/controllers appeal to the courts against orders of the regulators?

Yes, while there is no formal review mechanism in the Privacy Act, decisions made and actions taken by the Privacy Commissioner are subject to merit review by the Administrative Appeals Tribunal and judicial review by the Federal Court or Federal Circuit Court.

40. Are there any proposals for reforming data protection or cybersecurity laws currently under review? Please provide an overview of any proposed changes and

how far such proposals are through the legislative process.

Higher Penalties

There is a current proposal before parliament to significantly increase the maximum civil penalty for serious or repeated interferences with privacy, from the current penalty of AUD2.22m (for corporate entities) to the greater of $10m, 3 times the value of any benefit obtained through the misuse of the information, and 10% of the company's annual domestic turnover.

Online Privacy Code

A Bill is also before parliament for the introduction of an online privacy code (**OP Code**). The proposed code will apply to "OP organisations", that is, organisations providing any of the following:

- social media platforms (which includes social networks, online dating, online content, online blog or forum sites, gaming platforms and online messaging platforms);
- data brokerage services which are services involving the collection of personal information for the purpose of on-supply; or
- "large online platforms" which is any business that collects personal information in the course of providing access to information, goods or services online (that is, by the use of an "electronic service") and has at least 2.5 million Australian end users (such as Apple, Google, Amazon or Spotify).

The online privacy code itself is yet to be developed but will be required to set out the ways in which OP organisations will comply with the following APPs (in sum):

- APP 1.4(c) which is the purposes disclosure requirement in a privacy policy;
- APP 5 which sets out obligations around collection notices; and
- APP 3 and APP 6 which deals with the seeking of consent for collection, use and disclosure of personal information.

The OP Code will also require organisations to take reasonable steps (if any exist) to cease using an individual's personal information if they request it to do so. This appears to be similar to the "right to be forgotten" which is included in the European Union's GDPR but stops short by limiting the steps required to be taken by reasonableness.

The OP Code will also need to address how organisations interact with children, including, in respect of social media platforms specifically, an express fairness obligation and the requirement to obtain parental/guardian consent for the collection, use or disclosure of personal information for anyone under the age of 16 years.

Privacy Act review

On 12 December 2019, the Attorney-General announced that the Australian Government would conduct a review of the Privacy Act. The review was announced as part of the government's response to the Australian Competition and Consumer Commission's Digital Platforms Inquiry, which was primarily an inquiry into the practices of large online platforms operated by Google and Facebook.

In October 2021, the Attorney-General's Department released a Privacy Act Review Discussion Paper. The discussion paper contemplates the following reforms:

Change	Details on Proposed Amendments
Definition of personal information	Definition of personal information broadened to include “technical information”
Notice of collection	Express requirement that privacy notices be clear, current and understandable
Consent to collection, use and disclosure	Update definition of consent to be a voluntary, informed, current, specific, and an unambiguous indication through clear action
Standardised Notice and Consent	Suggestion that standardised privacy notices or consent with standardised layouts, wording and icons could be introduced in a Privacy Code
Additional requirements for collection, use and disclosure	Requirements for collection, use and disclosure of personal information to be “fair and reasonable”
Replace “de-identified” with “anonymous” for information not caught by Privacy Act	Increase standard from “de-identified” to “anonymous” for information to no longer be considered “personal information” that is caught by the Privacy Act
Right to object / withdraw consent	A right for individuals to object or withdraw consent at any time to the collection, use or disclosure of their personal information
Right to erasure of personal information	A right for individuals to request erasure of personal information under specific circumstances
Restricted Practices	Introducing requirements for entities to take reasonable steps to identify and mitigate privacy risks in relation to certain restricted practices
Pro-privacy defaults	2 options proposed: 1) (Strict) Pro-privacy settings selected by default, which means entities must pre-select the most restrictive privacy settings; 2) (Less strict) Easily accessible privacy settings, which means entities must make it easy to set privacy settings to the most restrictive, without jumping through any hoops
Additional protections for children	Amend the Privacy Act to require consent to be provided by a parent or guardian where a child is under the age of 16 (interestingly, this generalises similar provisions in the proposed OP Code discussed above)
Direct right of action	Creation of a direct right of action for individuals or groups of individuals in respect of whose privacy has been interfered
Statutory tort	Four options proposed, ranging from the introduction of a statutory tort for invasion of privacy to not introducing a tort and allowing common law to develop instead
Overseas data flows – Certification	Introduce a mechanism to prescribe and certify countries with substantially similar privacy laws as Australia, with the result that certain privacy obligations do not apply when disclosing information to those countries

Mandatory Ransomware Reporting

The Commonwealth Department of Home Affairs has published a Ransomware Action Plan which sets out the Government’s intention to introduce mandatory reporting obligations in the event organisations experience a ransom attack. This would apply to businesses with annual revenue in excess of AUD10,000,000 and would require (verbal) notification within 12 hours if the organisation experiences an attack with potentially significant impact.

Draft legislation for this has not been provided (as at April 2022).

Contributors

Simon Burns
Partner
sburns@gtlaw.com.au

Melissa Fai
Partner
mfai@gtlaw.com.au

Rebecca Dunn
Partner
rdunn@gtlaw.com.au

Mark Ferguson
Lawyer
mferguson@gtlaw.com.au