Privacy Reform - Consultation Paper

This Australian Government is considering a further package of reforms as the next stage of uplifting Australia's privacy laws, following the *Privacy and Other Legislation Amendment Act 2024* (Cth). The package includes the *Privacy Amendment (Personal Data Protection) Bill 2026* (Bill), which contains draft provisions for a range of proposed reforms to the *Privacy Act 1988* (Cth). The package includes roughly 40 proposals, including some that were proposals from the Privacy Act Review and some additional proposals:

- 25 Privacy Act Review proposals that uplift privacy protections
- 5 Privacy Act Review proposals that are designed to clarify and simplify obligations
- 4 additional measures to further simplify current obligations, and
- 7 additional measures to improve the efficiency of the privacy regulator (the Office of the Australian Information Commissioner (OAIC).

In addition to the measures included in the Bill, this consultation seeks feedback on proposed measures under development to:

- support the more efficient administration and enforcement of the Privacy Act by the OAIC, and
- address privacy issues arising from emerging technologies, including wearable surveillance technologies (such as smart glasses and ear buds) and connected vehicles.

Together, the measures in the Bill and the other proposed measures outlined in this consultation paper seek to strengthen Australia's privacy framework by providing stronger safeguards for individuals, greater clarity and certainty for regulated entities, and more effective administration and enforcement of the Privacy Act.

The Bill includes draft legislative provisions for a range of reforms to simplify and update the Privacy Act, including:

- **modernising and clarifying core definitions**, including personal information, sensitive information, de-identified, collects, consent, and disclosure
- **simplifying and strengthening requirements for the handling of personal information**, including through:
  - replacing complex and unclear obligations with a single **'fair and reasonable' test** for the collection, use and disclosure of personal information
  - **refining and strengthening consent requirements**, ensuring consent is required where it is most meaningful including for the collection of sensitive information or to trade personal information
  - enabling the appropriate handling of personal information through **permitted general situations** and **consent exceptions**
  - **simplifying notification requirements** to support genuine transparency, and
  - clarifying **direct marketing rules**, including the scope of activities covered by the rules and requirements relating to opt-out requests

- strengthening and clarifying requirements for **data security and minimisation**, and responses to **data breaches**
- introducing a right for individuals to request the **erasure of personal information** held by large digital platforms, and an exception where compliance is **technically impossible or infeasible**
- supporting research and innovation by **simplifying research exceptions** and facilitating the handling of personal information for ethically approved human research, and
- reducing unnecessary and confusing obligations for **processors** of personal information.

These reforms are intended to deliver three key outcomes: better privacy protections for Australians, greater certainty for businesses and other entities, and a stronger and more efficient privacy regulator.

Format of consultation paper

Where draft legislative provisions have been included in the Bill, this consultation paper seeks feedback on how those provisions would operate in practice. Specific consultation questions have been identified in relation to measures to address privacy issues arising from emerging technologies. The consultation is primarily focused on the practical operation and implementation of the proposed measures, including operational issues, operational considerations and compliance impacts.

The consultation paper does not identify in every instance where a provision preserves or merely clarifies a requirement already existing under the Privacy Act. References to the existing framework are included where they assist in explaining the practical operation or effect of a proposal. However, some provisions preserve existing requirements without this being expressly stated.

For proposed measures where a draft provision is not included, the consultation paper sets out the proposed approach and seeks stakeholder feedback to inform their further development.

Consequential amendments, and application and transition provisions, and commencement periods

Consequential amendments and application and transitional provisions have been included in the Bill in some but not all cases, to assist stakeholders in understanding the proposed operation of the reforms. Views on the optimal approach to these are welcome. Further consequential amendments and application and transitional provisions will be incorporated once settled.

Providing feedback

Stakeholders are invited to provide written submissions on the Bill, including any practical implementation issues and information on what practical impacts it would have. Feedback will help inform both the refinement of draft legislative provisions included in the Bill and the further development of proposed measures that remain subject to legislative and policy design.

Privacy Amendment (Personal Data Protection) Bill 2026

Schedule 1 - Core definitions

The amendments would update and clarify key Privacy Act definitions and concepts to better reflect contemporary digital environments, data practices and community expectations.

Personal information and reasonably identifiable

The definition of personal information would be amended to cover information that 'relates to' an individual who is identified or reasonably identifiable, and a new definition of reasonably identifiable is introduced.

Sensitive information

The amendments proposed would expand the definition of sensitive information, recognising that certain new categories of information warrant additional safeguards, including consent for collection unless an exception applies.

De-identified information

The definition seeks to clarify that de-identification is not a fixed state. Information is de-identified where it no longer relates to an identified individual, or an individual who is reasonably identifiable, having regard to the circumstances.

Collects

The proposed amendments make clear that personal information is 'collected' when an entity includes it in a record or generally available publication, regardless of the source from which, or how, the information is obtained. The amendments also clarify when entities will be taken to collect sensitive information that is derived from other personal information, regardless of whether the entity makes a separate record of that sensitive information.

Disclosure

The amendments would introduce a definition of disclosure based on whether an entity makes personal information accessible to another person or body. This provides greater clarity about when disclosure occurs, including where personal information is transmitted or stored overseas.

Consent

Proposed amendments to the definition of consent provide that it must be voluntary, informed, current, specific, and unambiguous. This will help ensure individuals have genuine choice and control over the handling of their personal information. The amendments also provide greater flexibility for certain human research projects where specified safeguards and ethical oversight requirements are met.

Personal Information	
Replace 'about' with 'relates to'	The definition of personal information would be amended by replacing the requirement that information be 'about' an individual with the requirement that it 'relates to' an identified or reasonably identifiable individual. In the definition of personal information, 'relates to' signifies the degree of connection required between information and an individual for the information to fall under the scope of the Act. The phrase bears its ordinary meaning and clarifies that while the individual need not be the sole or dominant subject of the

Personal Information	
	information, there must be a sufficient connection between the information and the individual in the circumstances. Information may 'relate to' an individual because of its nature, including where it 'says something' about the individual or their activities, characteristics, behaviour, circumstances, movements, preferences or interactions. Information may also relate to an individual because of the context in which it is collected, used or disclosed, including where it is used, or is capable of being used, to inform or influence actions or decisions which affect the individual. For example, a building inspector prepares a report on a property which indicates storm damage to a commercial property. In that context, the inspector's name and contact details will be information that relates to the inspector, but the report's findings are information that relates to the property, not the inspector. However, if a regulator later reviews the report in the context of an investigation into allegations of negligence by the inspector, the report's findings will become information that relates to the inspector. Whether information relates to an individual depends on the nature of the information and the purposes for which it is handled. Information will not relate to an individual merely because it has a tenuous, remote, incidental or trivial connection to them.
Note to clarify identifiability (Note 1)	The note seeks to clarify that an individual may be identified or reasonably identifiable even if their name or legal identity is not known where the information enables them to be recognised, singled out or otherwise treated as a distinct individual in practice. The examples in the note are non-exhaustive and are intended to assist entities in assessing whether an individual is identified or reasonably identifiable. Whether this threshold is met depends on the totality of the information and the circumstances in which it is held.
Definition of reasonably identifiable	The amendments would insert a definition of 'reasonably identifiable'. An individual is reasonably identifiable where, in the circumstances, they could be identified by combining the information with other information or opinions that are reasonably available to the entity. This assessment is objective and considers practical factors such as the availability of other information, technical feasibility, the time, cost and effort required to identify the individual, and any controls on access, use or re-identification. In assessing reasonable identifiability, foreseeable re-identification risks must be considered, including whether information could be combined with other information and the effectiveness of measures designed to prevent re-identification.

Sensitive Information	
Replace 'about' with 'relates to'	Consequential amendments would be made to the definition of sensitive information to replace 'about' with 'relates to' where appropriate, ensuring consistency with the amended definition of personal information. References to information 'about' a particular subject matter are retained where they describe the nature of the information itself. However, references to information 'about an individual' are generally replaced with references to information 'that relates to an individual' to ensure consistency with the amended definition of personal information.
Precise geolocation tracking data	The proposed amendments insert a definition of 'precise geolocation tracking data' as a type of sensitive information. The definition applies to personal information generated by or derived from a device or technology that identifies an individual's specific location to within a radius of 500 metres and is collected and held by reference to the individual's location over time. The definition is intended to capture information that enables tracking, monitoring or analysis of an individual's location over time. It is not intended to extend to one-off disclosures of location information, or to less precise location data (for example city location).
Genomic information	The proposed amendments include 'genomic information that relates to an individual' as a type of sensitive information. Genetic information is already included in the definition but, to avoid doubt, genomic information is included specifically. Genomic information may include findings about an individual's genetic characteristics, biological relationships, or potential health risks. Consequential amendments are made to the definition of health information to include 'genomic information' to ensure consistency.

De-identified information	
Definition of de-identified	The amendments would revise the current definition to provide that information is 'de-identified' where, in the circumstances, it does not relate to an individual who is identified or reasonably identifiable. Whether information is de-identified may depend on the context. Information that has been subject to de-identification techniques may nonetheless remain personal information where an individual can be identified or is reasonably identifiable through the combination of the information with other reasonably available information. The proposed amendments recognise that de-identification is not a static condition, having regard to factors such as technological developments, data availability and the effectiveness of technical and organisational measures to avoid re-identification.

De-identified information	
	The amended definition would work in conjunction with the obligation on entities in Australian Privacy Principle (APP) 11 to take reasonable steps to secure and destroy personal information, including by managing foreseeable risks that de-identified information may be able to be re-identified over time.

Collects	
Meaning of collects	The amended definition would provide that an entity collects personal information when it includes that information in a record or generally available publication, regardless of the source from which, or means by which, the information is obtained. This amendment and accompanying note recognise that personal information may be obtained from the individual to whom the personal information relates, from a third party or publicly available source, or may be generated or derived through means such as data analysis, artificial intelligence or other technological processes.
Collection of sensitive information that can be derived from personal information	The amended definition would clarify that an entity is not taken to collect sensitive information simply because it collects personal information from which sensitive information can be derived. This ensures that the obligations applying to the collection of sensitive information do not arise solely because the personal information is capable of revealing a sensitive attribute. However, where an entity collects personal information from which sensitive information can be derived, it may be taken to collect the sensitive information before that information is separately recorded. If the personal information is collected for a purpose that involves using or disclosing it as sensitive information, the sensitive information is taken to be collected at the same time as the personal information. Otherwise, it is taken to be collected when it is first: • used or disclosed as sensitive information, or • separately recorded, whichever occurs first. For example, an entity collects information that a person has ordered a halal meal for the purpose of processing a meal order. The meal order is not sensitive information merely because the entity could use it to derive the person's religious beliefs. However, the entity later uses the person's meal order to derive information about the person's religious beliefs in order to send marketing to them about a religious festival. The entity is taken to collect the sensitive information when it first records the derived religious beliefs, or uses or discloses them, whichever occurs first. References to the use or disclosure of sensitive information include the use or disclosure of personal information from which sensitive information can be derived, where the circumstances indicate that the information is being used or disclosed as sensitive information. Whether this threshold is met will depend on

Collects	
	the context. The mere use or disclosure of personal information from which sensitive information could be derived does not, by itself, mean that sensitive information is being used or disclosed.

Disclosure	
Definition of disclosure	The amendments would insert a definition of 'disclosure' which makes clear that, for the purposes of the Act, this occurs when personal information is made accessible to another person or body. Where an entity makes personal information accessible to an external third party, the amendments clarify that it is disclosed, regardless of whether the entity retains a level of control over it. Generally, making personal information accessible *within an entity* will constitute a use, while making it accessible *to a person or body outside the entity* will constitute a disclosure. By contrast, the mere transmission or storage of personal information, including overseas, will not constitute a disclosure unless the information is made accessible to another person or body. The disclosure may be to any person or body (irrespective of whether the body is regulated under the Privacy Act) and may occur by any means and does not require an intention to disclose the information.

Definition of consent	
Definition of consent	**Voluntary** means an individual must have a genuine opportunity to provide or withhold consent. Examples of practices that would most likely not be 'voluntary' include bundled consent (where an individual must consent to multiple information handling practices through one mechanism) and deceptive or misleading practices, including user interfaces that make it unreasonably difficult for an individual to avoid giving consent. Consent may still be voluntary where it is required to access particular features or elements of a good or service. **Informed** means an individual must have enough information to understand the consequences of providing or withholding consent, and what they are consenting to. **Current** means consent must relate to the current circumstances or information handling practices. The requirement is not intended to prescribe a period within which consent must be renewed. However, if circumstances have materially changed, consent which was previously provided by an individual may no longer be relevant. It also means consent has not been withdrawn by the individual.

Definition of consent	
	Specific - the consent must be sufficiently precise in the context of the proposed information handling. This is designed to guard against overly broad or 'bundled' consents, or seeking consent for undefined future uses of personal information. **Unambiguous** means an individual's choice must be clear. Seeking consent through preselected settings or pre-ticked boxes would likely not be sufficient. Consent may still be implied where it can be clearly inferred from the individual's conduct and the purpose of the consent is obvious from the context.
Definition of consent - collection of sensitive information for research	
Research exception	For human research projects that are ethically reviewed, approved and monitored in accordance with the National Statement on Ethical Conduct in Human Research, consent would not be required to satisfy the 'current' or 'specific' elements of the definition of consent.

Schedule 2 – Handling of personal information

Part 1 – Fair and reasonable handling of personal information; consent and notice requirements

Repeal of previous obligations to ensure a simplified framework

Existing APPs 3, 4 and 6 would be replaced with a new framework for the collection, use and disclosure of personal information. This framework is centred around a new test which permits the handling of personal information only where it is fair and reasonable in the circumstances, with reference to a non-exhaustive list of factors. There are exceptions where a permitted general or health situation applies or the information handling is required or authorised by law. The new framework applies key principles of data protection in a simpler and less prescriptive way.

Under the proposed new framework, collection, use and disclosure obligations are located in a single principle. Requirements to obtain consent to collect sensitive information and to trade personal information are in a separate principle. The exceptions to current collection, use and disclosure obligations are retained as permitted general situations.

Fair and reasonable test

The proposed fair and reasonable test includes a number of legislated factors to which entities must have regard to determine if their personal information handling satisfies the test. The OAIC will also provide guidance, including practical examples, to assist entities. An entity would not be required to satisfy every legislated factor for a particular act or practice to be fair and reasonable. Instead, these factors would need to be considered as part of a holistic assessment in the circumstances. No single factor will determine whether a particular collection, use or disclosure is fair and reasonable. This principles-based test will enable privacy protection to adapt to evolving technology and practices.

Consent to collect sensitive information or trade personal information, with exceptions

These amendments would make clear that an organisation must not collect sensitive information from an individual, or trade their personal information, without consent unless an exception applies.

APP entities are already generally required to obtain an individual's consent before they collect sensitive information. The amendments introduce two new exceptions. The collection of sensitive information will still need to be fair and reasonable in the circumstances.

Notice requirements

The proposed amendments simplify notification requirements when collecting personal information and require that details provided to individuals are relevant, clear and concise.

Repeal of previous obligations	
Collection obligations	
Collection limitation	The existing collection limitation requirement in APP 3 would be replaced by the fair and reasonable test, which provides a clearer standard while retaining the concepts of legitimacy, necessity and proportionality that underpin the current

Repeal of previous obligations	
	‘reasonably necessary’ test. In applying the test, entities will need to consider whether their purpose could be achieved by collecting, using or disclosing less personal information, or information that is not personal information. This ensures that data minimisation is considered throughout the information handling lifecycle, rather than only at the point of collection.
Lawful and fair means	The proposed new framework removes the requirement to collect information by lawful and fair means and instead prohibits collection, use and disclosure of personal information unless it is fair and reasonable in the circumstances, and lawful. Under the new test, the *means* and *purpose* of collection, use and disclosure must both be fair and reasonable in the circumstances.
Direct collections	There would no longer be an express requirement for personal information to be collected directly from an individual unless unreasonable or impractical or another exception applies. However, whether personal information is collected directly from the individual, or some other way, will be relevant to assessing whether the collection is fair and reasonable. This reflects the modern reality that personal information is routinely obtained from sources other than the individual, including other entities, publicly available sources, and by generating and deriving information. Entities will need to assess whether their collection of personal information is fair and reasonable by considering factors such as an individual’s reasonable expectations, transparency, genuine choice, and proportionality. Depending on the circumstances, collecting personal information from a source other than the individual may be reasonably expected and enable more up-to-date information to be collected in a way that is less burdensome for the individual.
Solicited and unsolicited personal information	The express differential treatment of solicited and unsolicited personal information would be replaced with the requirement that collection of personal information, however it occurs, must be fair and reasonable in the circumstances. While the same test applies regardless of how an entity comes into possession or control of personal information, the circumstances of collection will be relevant to whether it is fair and reasonable (including via the legislated factors which refer to an individual’s reasonable expectations, transparency and genuine choice).
Use and disclosure obligations	
Primary and secondary purposes	Although purpose specification and use limitation are not expressed as standalone requirements within the fair and reasonable test, the proposed test gives effect to those concepts through its legislated factors. A use or disclosure for a purpose that arises after collection is less likely to be fair and reasonable where it falls outside an individual's reasonable expectations, lacks transparency, or occurs in circumstances where the individual has not been provided with genuine choice. The purposes for which information was originally collected will therefore remain central to the assessment of subsequent uses and disclosures.

Repeal of previous obligations	
Consent for secondary use and disclosures	There would be no express requirement to obtain consent for unexpected or unrelated secondary uses and disclosures of personal information. Entities will instead need to assess whether, in the relevant circumstances, their actions are fair and reasonable, including by reference to whether the individual has had genuine choice about how their information is being handled, alongside other legislated factors. Consent may continue to be a mechanism that entities use to provide individuals with choice, but it will only be valuable if meaningful. Whether choice is genuine will depend on the information provided to an individual and the options available to them.

Fair and reasonable handling of personal information	
Legislated factors	
Reasonable expectation	This factor requires entities to consider what a reasonable person in the individual's circumstances would expect. It is relevant to assess whether the purpose for handling personal information is legitimate, whether it existed at the time of collection or arose later and whether it is appropriate. Entities do not need to consider an individual's personal or subjective expectations. Reasonable expectations are determined by the context of the relationship and broader community standards, as well as the information an entity provides. Reasonable expectations will vary depending on the context, including whether the entity is providing a one-off transaction or an ongoing service, and the nature of the relationship with the individual. Where there is a significant power imbalance or an entity provides an essential service, a reasonable person is less likely to expect their information to be used beyond what is necessary for the entity to perform its core functions or activities. While information handling is less likely to be reasonably expected if the individual is unaware of it, a practice does not necessarily become reasonably expected simply because it is described in a collection notice or privacy policy. Equally, a practice may be reasonably expected even if it has not been expressly notified. Transparency and reasonable expectations are related but distinct. What a reasonable person would expect in the circumstances also depends on the nature of the personal information, including whether it is publicly available and the circumstances in which it became public.
Relationship to an entity's functions or activities	This factor considers the connection between an entity's functions or activities and its handling of personal information. An entity's functions and activities will generally be described on its website and in corporate documents, advertising, product disclosure statements, and communications with clients and customers. The handling of personal information does not need to be *essential* for an entity's operations to be *related to* its functions or activities, but there must be a clear connection. Where such a connection exists, this will weigh in favour of

Fair and reasonable handling of personal information	
	the information handling being fair and reasonable. Where the purpose for information handling is related to an entity's functions or activities it must then consider whether the way it pursues that purpose is fair and reasonable, given the other factors. This factor is particularly relevant where personal information is used or disclosed for a purpose other than the purpose/s for which it was originally collected. Rather than relying solely on consent, whether the use or disclosure is related to the entity's functions or activities will be relevant. Where information handling is not related to the entity's functions or activities, reasonable expectations and genuine choice become especially important. Such information handling that is neither reasonably expected nor the subject of genuine choice is not likely to be fair and reasonable.
Transparency	This factor requires consideration of whether the information provided by the entity would enable a reasonable person to understand why their personal information is being handled and how it will be handled. This may be achieved through a collection notice, noting that entities already have an obligation to take such steps (if any) as are reasonable in the circumstances to provide collection notices to individuals. However, it may not always be practicable to provide a collection notice or ensure that an individual is aware of matters outlined in a notice, such as where the entity cannot contact them. Even in these circumstances, transparency remains relevant to assessing whether the information handling is fair and reasonable. An entity is not automatically transparent simply because information is included in a privacy policy, particularly if the policy is lengthy or unclear. Entities should consider whether the purpose and method of handling personal information are explained in plain language, provided in a timely manner, and are readily accessible to individuals. As a general rule, entities should be transparent about the purpose and method of information handling before collecting, using or disclosing personal information. However, this will not always be practicable, and in some cases no information may be provided to the individual. In those circumstances, the information handling may still be fair and reasonable, including where it would be reasonably expected.
Data minimisation	This factor recognises that, even when pursuing a legitimate purpose, entities should exercise restraint in their handling of personal information and assess what amount of personal information is required to achieve the intended objective. In considering whether less personal information could be handled, entities should have regard to both the nature and volume of the information, including its sensitivity. This requires consideration of what the information may reveal about an individual or group of individuals. Some information may create

Fair and reasonable handling of personal information	
	significant privacy risks even if it does not meet the definition of 'sensitive information' in the Act. Entities must also consider whether their purpose can be achieved without personal information, including through the use of de-identified information. Where a purpose could be achieved with less personal information or de-identified information, the entity should be able to justify why handling additional, or more sensitive, personal information is fair and reasonable, having regard to the other factors. This balancing approach helps ensure that higher-risk information handling is supported by stronger justification and safeguards.
Genuine choice	This factor requires entities to consider the degree of control an individual has over the collection, use or disclosure of their personal information. Whether choice is genuine will depend on factors such as how easy it is to exercise, the information provided to the individual, and whether meaningful alternatives are available. Choice will not be genuine where individuals are presented with 'take it or leave it' terms, would suffer detriment for refusing, or are influenced through the use of dark patterns. Where personal information must be collected, used or disclosed to provide a particular good or service, an individual's decision to obtain that good or service will be relevant to whether they have exercised genuine choice. However, where essential goods or services are involved, or individuals have limited alternatives, other factors, particularly reasonable expectations, may be more important. Genuine choice can be supported through measures beyond consent requests, such as accessible and easy-to-use privacy settings, clear opt-out mechanisms, and information fields that are clearly identified as optional. However, the absence of choice does not necessarily mean that information handling is not fair and reasonable. In some circumstances, the collection, use or disclosure of personal information may still be fair and reasonable when the other factors are taken into account.
Impacts to the individual and proportionality	This factor recognises the impact that information handling can have on individuals and requires entities to ensure those impacts can be justified in light of the benefits of the activity for the individual or the entity. Its purpose is to protect individuals from information handling that has an undue impact on privacy or causes unjustified harm. In assessing whether information handling is proportionate, entities must consider the potential impacts on an individual, the steps taken to mitigate those impacts, and the expected benefits. This assessment should take into account both the likelihood and severity of any harm. The greater the risk of harm, the stronger the justification and safeguards that are required. Particular regard must be given to circumstances in which the entity is likely to handle information about individuals experiencing vulnerability, or where the activity may have a significant effect on those individuals.

Fair and reasonable handling of personal information	
	Relevant impacts may include unlawful discrimination, unfair or deceptive treatment, financial, physical or reputational injury (including identity theft and threats to life or safety), unwarranted intrusion into private life, deprivation of rights and freedoms, loss of autonomy and psychological or emotional harm. When assessing benefits, entities should consider whether those benefits primarily accrue to the individual or the entity. Information handling is unlikely to be proportionate where there is a significant risk to individuals, and the entity is the primary beneficiary. Entities should also consider whether the same outcome could be achieved through a less privacy-invasive approach. If a less invasive option would achieve the same outcome, the more invasive approach may not be proportionate.
Best interests of the child	This factor recognises that children are particularly vulnerable to privacy risks and may be less able to understand the long-term consequences of how their personal information is handled. Where personal information relates to a child, the child's best interests must be a primary consideration when assessing whether the handling is fair and reasonable. When assessing whether personal information handling is in a child's best interests, relevant considerations may include the child's age, the nature of the service, the sensitivity of the information, and the potential benefits and risks of the information handling. This does not prevent entities from collecting, using or disclosing children's personal information, but as a primary consideration, the best interests of the child must be given significant weight when assessing whether information handling is fair and reasonable. This recognises that a child's interests may need to be balanced against other legitimate interests, including those of parents or guardians, other children, businesses, governments and the wider community.

Consent to collection of sensitive information or trading of personal information, with exceptions	
Consent to trade	
Definition of trading	The proposed definition of 'trade' is intended to capture the disclosure of personal information by an organisation for monetary or other consideration or for direct marketing purposes, subject to certain carve-outs. The reference to consideration adopts its meaning under Australian contract law and is intended to cover a broad range of arrangements in which personal information is disclosed as part of an exchange. This may include the transfer of shares, the exchange of customer lists, or other transfers of personal information for value. Disclosure 'for the purposes of direct marketing' is intended to be interpreted broadly and includes disclosures that support or inform direct marketing, even

Consent to collection of sensitive information or trading of personal information, with exceptions	
	where marketing is not the sole purpose. For example, this may include disclosures of cookies or pixels in programmatic advertising processes.
Carve-outs	There are four carve-outs from the definition of trade. Where a disclosure falls within a carve-out, it is not a trade and the consent requirement does not apply, although other obligations, including the requirement that information handling be fair and reasonable in the circumstances, may still apply. A disclosure is not a trade where: • it is necessary to provide a product or service requested by the individual, including where the disclosing organisation receives a commission for facilitating that service • it is incidental to the sale, acquisition or transfer of a business or part of a business, including disclosures made to facilitate the transaction, provided the disclosure of personal information is not the substantial purpose of the transaction • personal information is disclosed to a processor acting on behalf of a controller organisation and only in accordance with its documented instructions, or • it is necessary to prevent, detect, investigate or remedy unlawful activity or serious fraud related misconduct, including where the recipient provides fraud prevention or detection services.
Requirement for consent to trade	An organisation must not trade in personal information without the individual's consent unless an exception applies. The exceptions to consent to trade in personal information are also exceptions to the requirement for a disclosure to be fair and reasonable in the circumstances. (This means that if an organisation satisfies one of these exceptions it would apply to both requirements).
Exception for collection from a publicly available document	
Publicly available document	An APP entity would not be required to obtain an individual's consent when collecting sensitive information from a publicly available document as defined in Schedule 2. The definition of *publicly available document* is intended to be broad. *Document* has the meaning given in the *Acts Interpretation Act 1901* (Cth) and includes any record of information, such as audio recordings, photographs, videos and written material. A document may be publicly available even where there is a barrier to access such as a payment, registration, or account creation, provided those requirements can be met by any ordinary member of the public. However, a document is not publicly available where access depends on a person possessing particular characteristics or qualifications not ordinarily held by members of the public.

Consent to collection of sensitive information or trading of personal information, with exceptions	
	This concept is broader than that of a *generally available publication*, which is limited to published materials such as registers, books, newspapers, magazines, articles, and reports. A publicly available document may also include other publicly accessible material, such as social media posts. Whether particular material is a publicly available document will depend on the circumstances. While entities will not be required to obtain consent to collect sensitive information from publicly available documents, these collections will still need to be fair and reasonable. Factors such as reasonable expectations, data minimisation and proportionality will be particularly relevant to this assessment.
Exception where collection is strictly necessary to provide or deliver requested good or service	
Strictly necessary	An APP entity would not be required to obtain an individual's consent to collect sensitive information where the collection is strictly necessary to provide or deliver a good or service explicitly requested by the individual. The exception applies only where the good or service cannot be provided in a less privacy-intrusive manner, including through the use of non-sensitive personal information. Where the collection relates to a child's sensitive information, the requested good or service must be necessary to protect the child from neglect or physical, mental, or emotional harm, or to support the child's physical, mental, or emotional wellbeing. This is intended to facilitate access to essential support services, including confidential legal advice, domestic violence support, and counselling. Any sensitive information collected under this exception may only be used or disclosed for the purpose of providing or delivering the requested good or service. The exception does not apply to direct marketing.

Notification of the collection of personal information	
Matters to be notified	The proposed amendments replace the current list of matters to be notified to individuals when their personal information is collected with the following: • the fact and circumstances of the collection, and • the purposes for which the entity intends to use or disclose the information. This ensures individuals are aware of relevant details about how, when and where their information is collected. This is particularly relevant where the collection may not be obvious to the individual. Individuals would also be aware of the intended purposes of the entity's use or disclosure of the personal information.

Notification of the collection of personal information	
Form of notification	The proposed amendments include new requirements about the form of notifications to make it clear that information provided to individuals must not be excessive, vague, ambiguous, or include irrelevant information that may obscure key matters or make them hard to understand. Entities will have flexibility to notify of matters beyond the specified matters in a clear and concise manner if this supports fair and reasonable information handling. It is proposed that notifications must be updated when entities' practices change, such as where personal information is collected using different methods and information is handled for new purposes.

Schedule 2 – Handling of personal information

Part 2 – Permitted general situations

The amendments clarify and expand the application of this permitted general situation to enable entities to take appropriate action to address unlawful and wrongful conduct, including financial abuse.

Permitted General Situation (PGS) Item 2 (PGS2)	
Scope of conduct	This change would amend PGS 2 by replacing 'misconduct of a serious nature' with 'wrongdoing of a serious nature'. The concept of wrongdoing is intended to be broader than misconduct and includes, but is not limited to, misconduct. Misconduct, as defined in section 6, generally refers to conduct occurring in the course of a duty, such as in an employment, professional, or official context. PGS 2 will continue to apply to such conduct. The amendment clarifies that PGS 2 may also apply to serious wrongdoing outside the concept of misconduct, including some forms of financial abuse. Wrongdoing may include conduct by a person acting in a private capacity. For example, PGS 2 may apply where an entity suspects a person is exploiting a customer's vulnerability or misusing an enduring power of attorney for personal gain. The scope of the amendment remains limited by the existing requirements of PGS 2. An entity may only collect, use, or disclose personal information if it has reason to suspect serious wrongdoing relating to its functions or activities and reasonably believes the handling is necessary to take appropriate action. Whether that belief is reasonable will depend on the circumstances, including whether the proposed information handling is proportionate to the suspected wrongdoing and whether less privacy-intrusive alternatives are available. PGS 2 continues to apply to conduct that has occurred, is occurring, or may occur. As a result, it may support proactive monitoring and risk detection activities where an entity has reason to suspect fraud or other serious wrongdoing relating to its functions or activities, even if no specific instance of wrongdoing has yet been identified.
Internal and external conduct	The proposed amendments also clarify that unlawful activity and wrongdoing may relate to an entity's functions or activities *regardless of whether the person engaging in the conduct is internal to the entity* or otherwise owes a duty to the entity. This clarification is intended to address uncertainty arising from the Explanatory Memorandum to the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth).

Schedule 2 – Handling of personal information

Part 3 – Direct marketing

APP 7 would be replaced with a simplified direct marketing framework, supported by a clear, technology-neutral definition of direct marketing. The framework sets out simplified obligations for direct marketing communications and operates alongside the requirement that the collection, use, and disclosure of personal information must be fair and reasonable in the circumstances.

The framework retains the requirement for a simple opt-out mechanism, provides flexibility for ad-supported services, and clarifies the application of direct marketing obligations in multi-party advertising arrangements.

The framework does not require consent for direct marketing, but entities must obtain consent to trade personal information.

Direct marketing obligations	
Activities captured by direct marketing provisions	
Definition of direct marketing	The proposed definition clarifies that *direct marketing* includes advertising or marketing material directed to an individual using their personal information, whether the individual is targeted individually or as part of a broader audience, segment, or cohort. This includes communications such as emails, text messages, telemarketing calls, targeted social media advertising, and online behavioural advertising based on personal information, including browsing history. The definition reflects the increasing use of profiling and audience segmentation and makes clear that direct marketing includes group-level targeting that relies on personal information.
Opt-out requirements	
Requirement to provide opt-out	As under the existing framework, it is proposed that organisations must provide individuals with a simple means of opting out of direct marketing communications. The new framework clarifies that this obligation rests with the organisation that makes the communication. Where multiple entities are involved, such as an advertiser and a social media platform, the platform will generally be responsible for the opt-out requirement unless it is acting solely as a processor.
Actioning opt-out requests	It is proposed that if an individual requests not to receive direct marketing, an organisation must take reasonable steps to give effect to the request (that is, stop sending it). The 'reasonable steps' qualification recognises that direct marketing may be sent through multiple accounts, devices or identifiers and organisations may not always be able to link them to the same individual. What constitutes 'reasonable steps' will depend on factors such as the size and resources of the

Direct marketing obligations	
	entity, technical feasibility, the time and cost involved, and the sensitivity of the information.
Information about opt-outs	Each direct marketing communication would need to include information on how an individual may request not to receive direct marketing communications from the organisation. How this information is provided will depend on the type of communication, for example it may include an opt-out link or instructions on how to manage ad preferences or settings. The information must be clear, concise, up-to-date and written in plain language. The information should not include irrelevant information that may obscure key matters or make them hard to understand.
Opt-outs for ad-supported services	
Definition of ad-supported service	An 'ad-supported service' is one that derives revenue from the making of direct marketing communications to individuals who use the service. In determining whether a service is ad-supported, regard is only had to revenue from the making of direct marketing communications, and not to revenue generated from sales of the goods or services marketed through those communications. Importantly, the definition applies at the service-level. Where an organisation provides multiple services and only one of them is an ad-supported service, the definition only captures that one service. The definition would not impose a minimum revenue threshold. A service may be an ad-supported service even if only part of its revenue is derived from the making of direct marketing communications. The relevant question is whether the making of direct marketing communications is a source of revenue for the service. However, the extent to which a service derives revenue from the making of direct marketing communications may be relevant to the application of other Privacy Act requirements, including the fair and reasonable test and whether the terms offered to individuals provide a genuine choice to continue using the service without receiving direct marketing communications.
Modified opt-out	The proposed new framework makes it clear that ad-supported services are not required to continue to provide the same service to individuals who request not to receive direct marketing communications from the service. Instead, ad-supported services can offer the service, or an element of the service, on different terms, provided those terms give the individual a genuine choice to continue using the service without receiving direct marketing communications. This provision recognises that some services derive revenue from making direct marketing communications, while requiring individuals to be given a genuine choice to continue using the service without receiving those communications. The service that can be provided on different terms refers to the advertising-funded service such as the social media platform or video sharing platform the user is on, not to products or services offered in the advertisements on that service. Whether the options provided to an individual enable them to exercise genuine choice will depend on the circumstances, including how easy it was to choose a

Direct marketing obligations	
	preferred option, the information provided to the individual to explain the options and the comparative value of the options. Choice would not be genuine if it was illusory or if the entity used dark patterns to influence an individual's decision. This is intended to draw upon similar principles to 'consent or pay' guidance in data protection regimes in the UK and the European Union. Where an ad-supported platform does not provide an individual with genuine choice not to receive direct marketing communications, the platform will need to comply with the requirement to take reasonable steps to action opt-out requests.
Intersection with other regimes	
Intersection with other regimes	Existing APP 7.8 would be replicated. However, the new direct marketing obligations would only regulate the making of direct marketing communications and apply in addition to the general obligations for collection, use and disclosure of personal information. This means that the exclusion for direct marketing communications regulated by certain other laws only affects the operation of the direct marketing obligations. The exclusion does not, of itself, affect the application of the broader Privacy Act requirements relating to the collection, use and disclosure of personal information, including the fair and reasonable test where applicable.

Schedule 3 – Data security

Part 1 – Notifiable Data Breaches

These amendments to the NDB scheme would strengthen entities' obligations in responding to data breaches, minimise the risk of harm to affected individuals, and ensure that individuals receive timely and sufficient information to equip them to take action to protect themselves.

The proposed amendments also clarify that entities have a positive obligation to take reasonable steps to contain a data breach, including to prevent or minimise the risk of serious harm to individuals.

Data breach obligations	
Definition of data breach	The definition would distinguish a 'data breach' from an 'eligible data breach'. A separate definition would clarify that obligations under Part IIIC to manage and contain a data breach may apply even if the serious harm threshold for an eligible data breach is not met.
Practices etc. to enable effective responses	Entities would expressly be required to take reasonable steps to implement practices, procedures and systems that enable them to respond effectively to data breaches and prevent or reduce harm to affected individuals. This will help ensure entities are prepared to respond to actual or suspected data breaches, including eligible data breaches, and can take timely action to prevent or reduce harm – including meeting any notification obligations under the NDB scheme. This provision would not be prescriptive. What constitutes reasonable steps will depend on the entity's circumstances, including its size, resources, and the nature of the personal information it handles. Measures that may assist entities to comply with this obligation include maintaining, regularly reviewing and testing a data breach response plan to ensure it remains effective. A failure to comply with this obligation will constitute an 'interference with the privacy of an individual'.
Obligation to mitigate harm	Entities would have a specific obligation to take reasonable steps to prevent or reduce harm arising from a data breach. As soon as practicable after becoming aware of reasonable grounds to believe or suspect that a data breach has occurred, an entity must take reasonable steps to protect affected individuals whose personal information may have been compromised. This obligation would apply to actual and suspected data breaches, including eligible data breaches, and requires entities to take steps to mitigate harm at the earliest opportunity. The obligation would be ongoing. Entities must continue taking reasonable steps as their understanding of the breach develops, including its nature, scope, the sensitivity of the personal information, and likely impact on individuals.

Data breach obligations	
	Examples of mitigation measures include disabling compromised accounts, containing unauthorised access to systems, notifying relevant third parties to assist in preventing harm, and providing individuals with information on how they can protect themselves. The steps an entity takes to mitigate harm arising from a data breach may constitute remedial action. Failure to comply with this obligation constitutes an 'interference with the privacy of an individual'.

Eligible Data Breach	
Definition of 'eligible data breach'	It is proposed that the definition of 'eligible data breach' be amended to distinguish a data breach from an eligible data breach. An eligible data breach will continue to be a data breach that is likely to result in serious harm to one or more individuals. The definition would also clarify when an individual is considered to be 'at risk' of an eligible data breach. This will provide a clearer threshold for entities to determine whether an individual is at risk.
Exception for remedial action	The amendments proposed would simplify and clarify the existing remedial action exception and reflect the new definition of a data breach. The amendment is not intended to change the operation of the exception. It will continue to apply where a data breach would be likely to result in serious harm, but remedial action prevents that harm. In those circumstances, the breach is not, and is taken never to have been, an eligible data breach. The exception applies in two situations: 1. where a data breach involves unauthorised access to, or disclosure of, personal information and remedial action is taken before serious harm occurs, and 2. where a data breach involves the loss of personal information and remedial action is taken before or after any unauthorised access or disclosure. For example, if hard-copy records containing personal information are lost but recovered before anyone accesses them, or an unauthorised person accesses a customer database, but the entity quickly secures the account before any information is copied, downloaded, altered or further disclosed.
Statement about an eligible data breach	
Overview	The amendments to the notification requirements for eligible data breaches would strengthen and clarify these requirements by introducing clearer timeframes to notify the Information Commissioner, expanding the information that must be included in notifications, and requiring entities to provide additional

Eligible Data Breach	
	information to the Commissioner as further details about an eligible data breach becomes available. The key changes to the requirements are outlined below.
72-hour notification period	The proposed amendments provide that an entity must, within 72 hours of becoming aware of reasonable grounds to believe that an eligible data breach has occurred, give the Information Commissioner a statement that notifies the Commissioner of the eligible data breach and sets out required content. The 72-hour notification period aligns with reporting timeframes in other relevant Australian frameworks such as the *Security of Critical Infrastructure Act 2018* (Cth) and the *Cyber Security Act 2024* (Cth). The introduction of the 72-hour notification requirement would not alter the obligation for assessment of suspected eligible data breaches. An entity that has reasonable grounds to suspect that there may have been an eligible data breach but has not yet established reasonable grounds to believe that an eligible data breach has occurred, must continue to take all reasonable steps to ensure that the assessment is completed within 30 days. Where it is impossible or impracticable to provide a complete statement within 72 hours, entities may submit an incomplete statement and provide outstanding information later. Failure to provide any statement within 72 hours may result in an infringement notice or compliance notice, and constitutes an interference with the privacy of an individual.
Include information in the statement	The proposed amendments set out the matters that must be included in a statement given to the Information Commissioner following an eligible data breach. These matters substantially replicate the existing requirements, with the addition of information about the entity's response to the breach, including steps taken or proposed to reduce harm to affected individuals. The purpose of the amendment is to provide affected individuals with more information about an entity's response to an eligible data breach, including steps to reduce harm. The amendment will not require disclosure of information that could compromise cyber security or response activities.
When an incomplete statement may initially be provided	An entity may give the Information Commissioner an incomplete statement if it is impossible or impracticable to provide a complete statement within the 72-hour period. Where an entity provides an incomplete statement to the Commissioner, it must also provide written notice stating that the statement is incomplete, identifying the matters that are missing, and explaining why it was impossible or impracticable to provide that information within the 72-hour period. Where an entity provides an incomplete statement, the entity must give the Commissioner written notice of any missing matters as soon as practicable. A failure to provide that notice constitutes an 'interference with the privacy of an individual'.

Eligible Data Breach	
Notice of material changes	It is proposed that where an entity becomes aware that a statement given to the Information Commissioner or in a subsequent notice contains a material error or there has been a material change to that information, the entity must give the Commissioner written notice of the change or correction as soon as practicable. A failure to provide that notice constitutes an 'interference with the privacy of an individual'. This provision recognises that information provided during a data breach investigation may change as further information becomes available.
Entity must notify eligible data breach	
Overview	The proposed amendments clarify the operation of the requirements for notifying individuals of eligible data breaches, ensure affected individuals receive timely and up-to-date information, and align the notification framework with the new 72-hour notification requirement and staged reporting arrangements. The key amendments are outlined below.
Notification	The proposed amendments will align the notification requirements with the new framework that permits entities to provide an incomplete statement to the Information Commissioner within 72 hours where it is impossible or impracticable to provide a complete statement. As individuals may initially be notified on the basis of that incomplete statement, entities will be required to also notify individuals of any subsequent notices. This will ensure individuals receive any additional information, updates or corrections as they become available. These requirements are reflected in three notification pathways: notification of all affected individuals, notification of individuals at risk of serious harm, and public notification where direct notification is not practicable.
When notification must be given	The proposed amendments clarify when affected individuals must be notified of an eligible data breach, including notification of initial statements and any subsequent updates or corrections. These amendments will ensure individuals receive information about an eligible data breach as early as possible, while recognising that entities may not have sufficient information to notify individuals at the same time as they notify the Information Commissioner.
No individual notification if remedial action taken	An entity would not be required to notify an individual if remedial action has been taken and, as a result, a reasonable person would conclude that serious harm to that individual is no longer likely. These provisions recognise that, where remedial action has effectively removed the risk of serious harm to a particular individual, notification to that individual may no longer be necessary.
Exception – inconsistency with secrecy provisions	
Overview	Technical amendments would update the notification framework while preserving existing secrecy exemptions. The amendments clarify that these exemptions apply

Eligible Data Breach	
	to the initial notification to the Information Commissioner and any associated notices.
Commissioner may direct entity to notify eligible data breach	
Overview	Technical amendments align the Commissioner's direction power with the amended notification requirements for eligible data breaches. This power provides an alternative notification pathway where the Information Commissioner becomes aware of an eligible data breach other than through a statement given by an entity. The Commissioner may direct an entity to provide a statement and notify affected individuals. The key amendments are outlined below.
Compliance with direction	The proposed amendments provide that the Information Commissioner may direct an entity to provide a statement within 72 hours or a longer period allowed by the Commissioner. The discretion to allow additional time recognises that the circumstances of eligible data breaches vary and provides flexibility where more time is reasonably needed to comply. Entities must notify affected individuals as soon as practicable after notifying the Commissioner. Where required by a direction, entities must also notify the Commissioner of any material change to, or material error in, the information contained in a statement. The amendments would preserve the existing provision that a failure to comply with a direction from the Commissioner constitutes an interference with the privacy of an individual.
Requirement to provide a complete statement	Where an entity is directed to provide a statement to the Information Commissioner, it must provide a complete statement that includes prescribed matters. The amendments ensure that the same core information is required whether a statement is provided voluntarily following an eligible data breach or in response to a direction from the Commissioner. Requiring a complete statement reflects that a direction is typically issued after the Commissioner has assessed the circumstances and determined that notification is necessary. In addition, by the time a direction is given, the entity will generally have had a greater opportunity to investigate the incident and gather relevant information than an entity notifying following an eligible data breach.
No notification obligations for individuals if remedial action taken	Entities would not be required to notify an affected individual if remedial action has been taken and, as a result of that action, a reasonable person would conclude that the unauthorised access or disclosure would not be likely to result in serious harm to the individual. These provisions align with the remedial action exception. They recognise that notification may not be required where remedial action eliminates the risk of

Eligible Data Breach
serious harm. However, notification remains necessary for individuals who are still at risk or whose information is involved in an eligible data breach.

Schedule 3 – Data security

Part 2 – Security of personal information

The proposed amendments strengthen and clarify the obligations in APP 11 by specifying requirements relating to the protection, destruction and de-identification of personal information. They require APP entities to be able to identify personal information to which APP 11.1 and 11.2 apply, consider whether to destroy personal information that is no longer needed for any purpose for which it may be used or disclosed under the APPs, and regularly evaluate the effectiveness of their compliance with APP 11.

Security of personal information	
Requirement to consider destruction of personal information	It is proposed that if an entity holds personal information that it no longer needs for any purpose for which it may be used or disclosed under the APPs, it must first consider whether the information should be destroyed. It must then take reasonable steps to either destroy the information or ensure it is de-identified. This requirement recognises that retaining de-identified information can still create a risk of re-identification and encourages entities to consider whether destruction is the more appropriate option. An entity may decide to retain information in de-identified form where doing so supports its functions or activities, such as research or statistical analysis. In those circumstances, the entity must take reasonable steps to ensure the information is de-identified. APP 11.3 retains the existing exceptions in APP 11.2(c) and (d).
Requirement to identify personal information	An entity must take any steps needed to ensure it is able to identify personal information to which APP 11.1 and 11.2 apply. The ability to identify personal information is necessary for compliance with APP 11. An entity must know what personal information it holds in order to protect that information appropriately, determine whether it is no longer needed for any purpose for which the entity may use or disclose the information under the APPs, and whether it should be destroyed or de-identified. APP 11.4(a) preserves the existing requirement currently contained in APP 11.3.
Ongoing evaluation of security and destruction measures	An entity must regularly assess the effectiveness of its compliance with APP 11, including the reasonable steps it takes to protect personal information from misuse, interference, loss and unauthorised access, modification or disclosure. This requirement also applies to personal information that is no longer needed for a purpose permitted under the APPs. Entities must assess the effectiveness of measures used to destroy or de-identify that information. Where information has been de-identified, this includes assessing whether it remains de-identified, whether re-identification risks are being appropriately managed, and whether retaining the information in de-identified form remains justified instead of destroying it.

Security of personal information	
	Regular assessment recognises that security measures and information handling practices may become less effective over time as technologies, business practices and privacy risks evolve. Ongoing evaluation helps ensure an entity's measures remain effective and appropriate.

Schedule 4 – Data access and erasure

Part 1 – Technically impossible or infeasible

These amendments to APP 12 would insert a new exception to the requirement to give access to personal information where, despite taking reasonable steps to give access to personal information, providing access remains unreasonable or impracticable due to technical impossibility or infeasibility. They also make structural amendments to APP 12 to improve clarity and readability.

Exception to access requests where technically impossible or infeasible	
Introduce exception to access requests where technically impossible or infeasible	This proposed amendment creates a new exception to the requirement for APP entities to provide individuals with access to their personal information. The exception would apply where an APP entity has taken reasonable steps to provide access, but doing so remains unreasonable or impracticable because it is technically impossible or infeasible. This is intended to cover situations where there are technical limitations on how the information is held, or where compliance would be unreasonable given the nature of the request and the information involved. An APP entity may rely on the exception only if it has first taken reasonable steps to provide access. This is intended to prevent entities from designing systems in a way that avoids access obligations. If an entity has deliberately designed its systems so that access is impossible, it is unlikely to have met the requirement to take reasonable steps. The exception would apply only to the extent that providing access is unreasonable or impracticable. This allows for situations where some, but not all, of the requested information can be provided. In those circumstances, the APP entity must provide access to any personal information that is not covered by the exception.
Refusals to give access and partial access to information	Existing requirements would be co-located to clarify APP entities' obligations when they refuse access to personal information. These amendments do not change the substance of the obligations. Entities must continue to provide written notice of the reasons for the refusal unless unreasonable to do so, and information about available complaint mechanisms. Existing APPs 12.5 to 12.10 would also be restructured to make clear that, where an APP entity relies on an exception, including the new exception for technical impossibility or infeasibility, it must still take reasonable steps to provide access in a way that meets the needs of both the entity and the individual. Including the phrase 'all or some of the personal information' would clarify that access may be refused only in part. This will address situations where some, but not all, of the requested information is covered by an exception. In those cases, an APP entity must provide access to any information not covered by the exception.

Exception to access requests where technically impossible or infeasible	
Manner of providing access	Under the proposed amendment, APP entities must provide access to personal information in the manner requested by the individual where reasonable and practicable to do so. The amendments would clarify that, where an exception to the access obligation applies, the entity is not required to provide access in the requested manner but must still consider providing access in a way that meets the needs of both the individual and the entity. The existing requirement to respond to requests within certain timeframes remains unchanged.

Schedule 4 – Data access and erasure

Part 2 – Right to erasure on large digital platforms

These proposed amendments introduce a right to erasure for individuals applying to 'large digital platforms' (LDPs) which will be inserted as a new APP.

Organisations that are LDPs would be required to destroy personal information they hold relating to an individual upon request, unless an exception applies. LDPs will also have to provide the individual with written notice of the outcome of their request within a reasonable period.

Organisations are LDPs if they provide or operate a digital platform and they meet either, or both, of the following criteria:

- *their gross revenue for the previous financial year is $500 million or more, or*
- *their platform has 2.5 million or more average monthly end users.*

Exceptions to the right to erasure are provided to balance circumstances where there is a public interest in the organisation retaining the personal information.

Right to erasure on large digital platforms	
Definition of a 'large digital platform'	A new definition of 'large digital platform' (LDP) would be inserted into the Privacy Act. An organisation will be an LDP if it provides a service that is either a social media service, relevant electronic service or designated internet service as defined in the *Online Safety Act 2021* (Cth) (OSA) and meets the gross revenue test, the end users test, or both. An organisation may also be prescribed as an LDP by regulation. The OSA definitions capture a broad range of online services, including social media, messaging, email, gaming, streaming and other online platforms. These definitions were adopted because they broadly capture the services intended to be within scope, while the 'gross revenue' and 'end users' tests narrow the range of organisations captured. **Gross revenue test** – an organisation that provides a service covered by the OSA will be an LDP if its business group had more than $500 million in gross revenue in the previous financial year, calculated in accordance with relevant accounting standards. The threshold is intended to capture organisations that are sufficiently large to meet the erasure obligations. The test applies to the gross revenue of the organisation's entire business group, including overseas members. This recognises that Australian revenue alone may not reflect an organisation's size or capacity to comply with the obligations. An organisation that meets the test in one financial year is an LDP for the following financial year and must reassess its status at the start of each new financial year. **End users test** – an organisation that provides a service covered by the OSA will be an LDP if the platform has an average of 2.5 million monthly end users in Australia during the previous financial year. An end user includes any individual who accesses the platform, whether or not they hold an account, or who accesses or purchases a service through the platform.

Right to erasure on large digital platforms	
	Using an annual average ensures the test captures platforms with a consistently large Australian user base rather than those experiencing temporary spikes in usage. In addition to the threshold tests, it is proposed that regulations may prescribe specific digital platforms or classes of platforms as LDPs. This is intended to capture platforms that do not meet the thresholds but nonetheless collect significant amounts of personal information and present heightened privacy risks. A platform may only be prescribed if it falls within the OSA definitions.
Introduce a right to erasure applying to large digital platforms	The proposed right to erasure would require LDPs to destroy an individual's personal information on request, unless an exception applies. If an exception applies to only part of the information, the LDP must still destroy the remaining information. The right complements the destruction requirements in APP 11 by allowing individuals to request and receive confirmation of destruction, giving them greater control and certainty over the personal information an LDP holds about them.
Exceptions	The proposed right to erasure is not absolute. It is subject to exceptions that protect public interests and certain legitimate interests of LDPs. An LDP bears the onus of establishing that an exception applies and, where required, notifying the individual of the outcome. Exceptions fall into three broad categories: • public interest exceptions, including law enforcement activities • legal interest exceptions, where destruction would be inconsistent with a law, court or tribunal order, or a contract with the individual, and • technical or circumstantial exceptions, including technical impossibility or infeasibility and requests that are frivolous or vexatious. LDPs would not be required to destroy personal information held solely in their capacity as a processor. However, personal information they control remains subject to an erasure request. An LDP may also refuse a request that is frivolous or vexatious. In that case, it is not required to action any part of the request. An LDP would not be required to destroy personal information where: • a permitted general situation or permitted health situation applies at the time of the request • an Australian law, or a court or tribunal order, requires the information to be retained • despite taking reasonable steps, destruction is technically impossible or infeasible, or • the information is strictly necessary to provide an ongoing good or service to the individual. The technical impossibility or infeasibility exception would apply only where reasonable steps have been taken but destruction remains unreasonable or impracticable. The ongoing service exception would apply where the information is

Right to erasure on large digital platforms	
	strictly necessary to maintain an existing relationship or deliver a continuing service to the individual.
Dealing with requests for destruction	The right to erasure would require an LDP to destroy requested personal information, except where an exception applies, and provide written notice of the outcome within a reasonable period. The notice must identify the information destroyed, explain any exceptions relied on, and outline available complaint mechanisms. This ensures individuals understand the outcome of their request and can challenge it if necessary.

Schedule 5 – Exception for research

Agencies and organisations currently need to rely on different exceptions and follow different guidelines when undertaking health and medical research. This approach has created confusion for researchers and barriers for research partnerships. The current exceptions cover a limited range of research activities and require researchers to obtain the highest level of ethics approval. These exceptions would be repealed and replaced with a single exception for human research, supported by a single set of guidelines.

Broader exceptions for ethically reviewed human research	
Scope of research	The proposed new exception would apply to 'human research', defined as research that is conducted with or about individuals that involves personal information. To rely on the research exception, research will need to be reviewed, approved and monitored in accordance with the National Statement on Ethical Conduct in Human Research (issued by the National Health and Medical Research Council) and comply with human research guidelines (made by the Privacy Commissioner). The National Statement sets out ethical requirements for the design, review and conduct of human research. A research proposal is only ethically acceptable when its potential benefits justify any risks involved in the research, including privacy risks to a participant. The definition of 'human research' is intended to be read broadly to ensure consistency with the National Statement. Broadening the scope of research covered by the new exception will facilitate a wider range of socially beneficial research, including research that addresses sensitive or complex issues, while ensuring that privacy risks continue to be managed through ethical review and compliance with the human research guidelines. To ensure privacy risks are managed, the Commissioner will have the power to limit the scope of research covered by the exception. For example, the guidelines could limit the exception to particular kinds of human research or impose additional requirements in relation to research that presents heightened privacy risks.
Exceptions from APPs	The current health and medical research exceptions would be replaced with a single research exception that applies to both organisations and agencies. Where the requirements of the exception are met, an act done in the course of human research will not breach the APPs.
Research guidelines	When relying on the exception, researchers will be required to comply with human research guidelines issued by the Privacy Commissioner. The guidelines will be developed in consultation with research stakeholders including the National Health and Medical Research Council, the Australian Research Council and Universities Australia. The new guidelines will be consistent with existing ethical requirements set out in the National Statement. This will balance the public interest in protecting privacy with the public interest in research that is likely to benefit society. It is intended that the new research exception will commence once the human research guidelines are in place.

Schedule 6 – Exception for information processors

It is proposed that where an APP entity handles personal information on behalf of another APP entity, primary responsibility for compliance with the APPs will generally rest with the entity that determines the purposes for which the information is handled.

Allocation of responsibility between controllers and processors	
Definition of 'controller'	A controller is an APP entity on whose behalf a processor handles personal information.
Definition of 'processor'	A processor is an APP entity that does an act or engages in a practice on behalf of a controller. To satisfy the definition, the entity acting as a processor must act in accordance with a controller's documented instructions and handle information only for the purposes specified in those instructions. The definition only applies where both entities in the relationship are APP entities. To preserve the current framework that applies to contracted service providers for Commonwealth contracts, the definition excludes these entities.
Processor exceptions	An act or practice of a processor acting on behalf of a controller will not breach the APPs or a registered APP code, except APP 1 and APP 11. Accordingly, processors will remain directly responsible for complying with APP 1 and APP 11.
Documented instructions	A controller-processor relationship only exists to the extent that a processor acts in accordance with documented instructions issued by a controller and for the purposes specified in those instructions. There is no prescribed format or template for instructions, but they must address the purposes for which the processor will handle information on the controller's behalf. Instructions would not need to prescribe the technical or operational means by which a processor will handle personal information. This recognises that processors may exercise technical and operational expertise when carrying out a controller's instructions.
Liability	Where a processor acts in accordance with a controller's documented instructions, the processor's acts are taken to be acts of the controller. Where an act or practice undertaken by a processor on behalf of a controller would breach a registered APP code or an APP (other than APP 1 or APP 11) if done by the controller, the controller would be treated as having committed the breach. The framework would apply only where the processor acts in accordance with the controller's documented instructions and for the purposes specified in those instructions. If a processor acts outside those instructions, it is not acting on behalf of the controller and the processor exceptions do not apply. In those circumstances, the processor remains directly responsible for compliance with any applicable APPs and registered APP codes. Responsibility for compliance will depend on the scope of the controller's instructions and whether the processor acted in accordance with those instructions.

OAIC powers and efficiency

OAIC powers and efficiency measures

The Bill is also intended to include measures to enhance the regulatory powers and efficiency of the OAIC as privacy regulator, including to:

- *clarify and uplift the Privacy Act's early dispute resolution framework, and*
- *improve the OAIC's case management and enforcement powers, including to address practical challenges with representative complaints processes.*

These measures are intended to help the OAIC prioritise its regulatory activities in response to increasing demand, a rapidly evolving digital environment, and growing community awareness of privacy rights. They will support more efficient management of privacy complaints and strengthen the OAIC's enforcement powers, enabling it to more effectively handle complaints, conduct investigations and secure enforcement outcomes.

Uplift dispute resolution requirements to facilitate early resolution of complaints

This measure would clarify requirements in the Privacy Act for individuals making privacy complaints, APP entities handling those complaints, and the OAIC's complaint intake processes.

Individuals would generally be required to first raise privacy concerns with the relevant APP entity before complaining to the OAIC, giving the entity an opportunity to resolve the matter. When making a complaint to the OAIC, individuals would also need to provide information about their prior engagement with the entity and the outcome of that engagement.

APP entities would be required to provide accessible complaint mechanisms, respond within 60 days, and provide written decisions setting out the outcome and available review options, including external dispute resolution pathways where relevant.

The Information Commissioner could require complaints to be lodged in a particular form, while retaining discretion to accept alternative formats. The OAIC's obligation to assist privacy complainants would be aligned with its obligations under the *Freedom of Information Act 1982* (Cth), supporting effective complaint intake while maintaining accessibility for individuals who require assistance.

Uplift powers to enforce complaint handling obligations

This measure would classify breaches of APP entities' new complaint-handling obligations as an 'interference with the privacy of an individual', bringing them within the OAIC's existing enforcement framework—including complaint investigations, determinations, civil penalties, infringement notices and compliance notices.

It would also clarify the Commissioner's ability to enforce determinations through court proceedings.

The changes would encourage APP entities to improve their complaint-handling practices, resolve more matters directly and at an earlier stage, and reduce the volume of complaints requiring OAIC investigation.

Enable more efficient management of representative complaints

This measure is intended to ensure that there is greater clarity in the way representative complaints are made to and handled by the OAIC.

The changes are directed at ensuring that there is uniformity in the concerns of class members to a representative complaint and that there is greater clarity in the case management powers of the Commissioner to allow the OAIC to more efficiently and effectively progress representative complaints. The changes:

- provide an express power for the Information Commissioner to effectively group, deal with and determine multiple complaints in a similar way to the power vested in the President of the Australian Human Rights Commission under section 46PF of the *Australian Human Rights Commission Act 1986* (Cth)
- clarify that the complaints of class members to a representative complaint must be about the same act or practice that may be an interference with the privacy of two or more individuals
- protect an individual's right to make a complaint on the substantive issues they wish to make a complaint on, by clarifying that the Commissioner can only amend the class members to a representative complaint and not the substance or subject matter of a representative complaint, and
- establish clearer requirements for notifying potential class members of representative complaints, including about individuals' right to withdraw from a representative complaint.

Conduct assessments of privacy protections in the *Online Safety Act 2021*

This measure is intended to clarify the OAIC's ability to oversee privacy protections associated with the Social Media Minimum Age scheme in the *Online Safety Act 2021*.

The changes would expressly empower the Information Commissioner to conduct assessments of how social media platforms collect, use, retain and destroy personal information for age-assurance purposes. This would provide the OAIC with a more efficient, educative and preventive regulatory tool that enables constructive engagement with regulated entities, promotes best-practice compliance, and reduces the need for more resource-intensive investigations and enforcement action.

Require persons to provide reasonable assistance to the Information Commissioner in connection with an investigation

This measure is intended to improve the efficiency and effectiveness of OAIC investigations by giving the Information Commissioner a broad power to require any person who is able to assist an investigation to provide reasonable assistance, in addition to existing powers to compel information and documents.

Similar powers exist in other regulatory frameworks – for example, section 19 of the *Australian Securities and Investments Commission Act 2001* (Cth).

The reform recognises that modern privacy investigations often involve complex digital systems and online services, where traditional evidence-gathering powers are inefficient and overly reliant on voluntary cooperation. The new power would enable the OAIC to obtain practical assistance, such as access to systems, accounts or other investigative support, where reasonable in the circumstances, while retaining safeguards including judicial review and defences for self-incrimination, legal professional privilege, protection of journalists' sources, and situations where compliance is impossible or unreasonable.

The measure would be supported by a civil penalty regime for non-compliance and would apply to both investigations and public inquiries, helping the OAIC access relevant information more quickly and reduce delays caused where parties do not voluntarily cooperate.

Clarifying reporting powers to the Minister on ongoing investigations

This measure would clarify the OAIC's ability to share information with the Attorney-General and other Ministers about ongoing privacy investigations by repealing subsection 43(8A) of the Privacy Act.

Subsection 43(8A) currently restricts the OAIC from briefing Ministers on investigations involving most private sector entities and may also impede compliance with the Legal Services Directions 2025, which require significant legal matters to be reported to government.

The changes are intended to remove ambiguity, align the OAIC's powers with comparable regulators such as the Australian Competition and Consumer Commission and eSafety Commissioner, and ensure the OAIC can appropriately inform government of significant legal, policy or public interest issues arising from ongoing privacy investigations.

Clearer defences to information gathering notices

This measure would replace the current broad and undefined 'reasonable excuse' defence for refusing to comply with OAIC information-gathering notices (section 66 of the Act) with a closed set of specific, defined defences. The aim is to improve regulatory efficiency and reduce disputes about whether documents must be produced.

The existing defence and related provisions would be replaced with defences based on:

- privilege against self-incrimination
- journalists' privilege
- legal professional privilege
- inability to comply due to genuine practical barriers, and
- situations where requested documents cannot be located despite reasonable searches being undertaken and documented.

The changes draw on comparable provisions in the *Competition and Consumer Act 2010* (Cth) and are designed to provide greater certainty for regulated entities and support more efficient enforcement of OAIC's information-gathering powers.

The changes would not affect other uses of the 'reasonable excuse' defence in the Privacy Act.

Addressing emerging technologies

The Government is conscious of community concerns about the increasing ability of emerging technologies, including smart glasses, to record discreetly in public and private spaces and collect people's personal information.

The Government is also focused on giving Australians the confidence to adopt AI responsibly while ensuring effective privacy safeguards, recognising that AI systems are becoming increasingly sophisticated in how they handle personal information.

The Privacy Act is intentionally technology neutral and principles based. It is designed to remain relevant as new technologies emerge. However, with the exception of a new statutory tort introduced in 2024, the Privacy Act does not apply to individuals acting in a personal capacity.

The statutory tort for serious invasions of privacy was designed to provide redress for serious invasions of privacy while permitting conduct that is justified in the public interest. The tort is intended to be technology-neutral and can apply to privacy harms arising from emerging technologies, including wearable surveillance technology such as smart glasses. Liability may arise for both individuals and corporations, depending on the circumstances, but individuals may be unaware of how the tort could apply to harms arising from wearable surveillance technologies.

Where an entity regulated by the broader Privacy Act collects and uses personal information through technologies like smart glasses, including photos, videos, audio recordings and/or AI-generated inferences, it must comply with privacy laws. This includes obtaining consent to collect sensitive information, such as biometric templates.

Several measures currently in the Bill will improve transparency, accountability and individuals' control over their personal information, and help to address the privacy risks associated with emerging technologies:

- **Modernised key Privacy Act definitions** to clarify that personal information is not limited to names and legal identifiers but can also include behavioural information and other data generated or collected by wearable devices, including smart glasses.
- **Clarifying the definition of collection** to ensure that personal information may be 'collected' regardless of where it came from or how it was obtained. This reform will ensure that inferences drawn by AI-enabled technology about an individual would be considered collection of information for the purpose of the Act.
- **Requiring information handling to be fair and reasonable in the circumstances**, considering factors such as the risk of harm and an individual's reasonable expectations of privacy based on the circumstances. This reform will require deployers and developers that collect personal information through wearable devices to implement safeguards and restrictions to ensure fair and reasonable handling and to limit the risk of harm to individuals.
- **Requiring meaningful consent before entities can trade personal information** to ensure consent is required to trade in personal information collected by wearable technology.
- **Classifying precise geolocation data as sensitive information** to ensure entities must obtain (meaningful) consent before this data can be collected.
- **Uplifted security and notifiable data breach requirements** to ensure information is destroyed when it is no longer needed and strengthen the actions entities need to take in response to data breaches.

- **Introducing a right to erasure on large digital platforms** will provide a clear pathway for individuals to request that their personal information be destroyed (noting this would only apply to large digital platforms).

The Government would welcome views on whether these proposals adequately protect the privacy risks associated with emerging technologies.

Questions for stakeholders

1. Are the **proposed** updated **definitions sufficient to address** the **risks** of **emerging technologies?**
2. Is the **definition of 'collection' sufficient**ly **flexib**le **to capture** information collected via **new technologies such as wearables?**
3. **To what extent can the reforms ensure that consent is meaningful**, given that **wearable** technologies compromise the **transparency of captures and uses** of **individuals**' personal information**?**
4. Are existing remedial options adequate, including to ensure that individuals whose privacy has been interfered with can seek removal of relevant content? If not, what additional measures should be considered (without duplicating existing powers)?
5. **To what extent will** the **existing or proposed measures** encourage **improved compliance?**