Privacy Amendment (Personal Data Protection) Bill 2026

Key Changes — Exposure Draft Summary

This note summarises the changes and practical impact of the proposed privacy reforms. The most significant changes are highlighted in blue.

Core definitions (Schedule 1)

Issue	Proposal	Practical impact	What remains unclear?

What is personal information?	The definition of personal information would be expanded:
	• to cover information that 'relates to' an individual (expanded from 'about' a person);
	• to broaden the meaning of 'reasonably identifiable' to cover situations where the information does not identify an individual but allows them to be '**recognised, singled out or treated as a distinct individual**' (individuation).
		• Personal information would cover information that:
		  • **infers** information about the individual or their activities, characteristics, behaviour, circumstances, movements, preferences or interactions (**even where it doesn't identify them**);
		  • **relates to** an individual because it is used to inform or influence actions or decisions which **affect the individual**.
		• The '**singling out**' approach could capture **online tracking technologies** that rely on unique identifiers (not linked to a known identity).
			• It is unclear whether the widened definition of PI will include **audience segments which are built upon anonymisation and inferences at scale** (as distinct from behaviours inferred about a particular audience member).

Collection	• PI could be 'collected' by drawing inferences from other information and includes **data analysis, AI or other technological processes**.	• This is a broader definition of 'collect' consistent with the recent changes to the APP3 guidance. • You may be collecting PI when undertaking **data analysis** to make inferences. • This broad definition of collection is likely to cover new technologies, such as **smart glasses, connected cars, home speakers and personal health devices**.	• Unclear whether 'collection' will take place when inferences are made from anonymised data.
Sensitive information	• An entity won't automatically be taken to have collected sensitive information simply because it collects PI from which sensitive information could be derived. • But, if the entity separately **uses or separately records the sensitive information** it will be collecting that information.	• You do not collect sensitive information just because you process information from which sensitive attributes can be inferred (e.g. halal meal order). • But, if you use that information to market a religious festival you are collecting the sensitive information (so would need consent etc).	

Issue	Proposal	Practical impact	What remains unclear?
	• Geolocation data (see below) and genomic information (including biological relationships or health risks) are specifically included as sensitive information.		
Precise geolocation tracking data	• A **new category** of sensitive information — 'precise geolocation tracking data' — would be introduced. • This would cover information that pinpoints an individual's location to **within 500 metres**.	• This becomes a new type of sensitive information requiring **consent** to collect. • This covers data that enables **tracking over time**, not one-off or less precise (e.g. city-level) location data. • Potential for significant impact for businesses with a location SDK in their apps	• Unclear whether this will impact on businesses using a location SDK in their apps for targeting and measuring (including footfall attribution). • The distinction between 'one-off' and 'tracking over time' may be tricky to apply in practice, as many uses will fall somewhere in between.
De-identified information	• 'De-identified' would be redefined so information only qualifies once it no longer relates to an identified or reasonably identifiable individual. • This depends on the context and may change over time.	• De-identification isn't a one-off, permanent status — **analytics datasets may become re-identifiable** as technology or available data changes, so ongoing risk assessments will be needed. • This obligation works alongside the existing obligation to secure and destroy PI (APP11) which will now include managing the **risk that de-identified information may be re-identified over time**. • As de-identification is not static, but can change over time, **it may be difficult for organisations to rely on de-identification**.	• The context specific definition may be hard to apply in practice, especially when entities may not be aware of all available technologies.
Consent	• Consent may be express or implied, but must always be **voluntary, informed, current, specific and unambiguous**.	• 'Bundling' consent it unlikely to be adequate (not voluntary or specific). • Interfaces that make it difficult for an individual to avoid giving consent are unlikely to be adequate (not voluntary). • It may be acceptable to request consent to access particular features of a service (but total denial of a service could be more problematic as it means the consent may not be voluntary). • Implied consent remains valid.	• The threshold of choice/voluntariness is unclear. • It is unclear how the requirement to give a consumer choice to access services (or part of a service) will work in practice.

Handling personal information (Schedule 2)

Issue	Proposal	Practical impact	What remains unclear

Fair and reasonable	• APPs 3, 4 and 6 would be replaced with a **new test** which allows the handling of PI only where it is **fair and reasonable in the circumstances**.
	• There is a list of factors to be taken into account including the individual's **expectation**s, the **transparency** provided, whether the objective could be **achieved with less information**, and whether the individual had a **genuine choice**.
	• **Where children are involved, their best interests must be a primary consideration**.
		• This is the key pillar of the new framework.
		• It replaces 3 APPs with a single test.
		• **Genuine choice** may require a change in business practice to enable users to access at least part of the service/product. It may also be achieved by **opt-out mechanisms** and **optional information fields**.
		• The **original collection purpose** remains central — the further an entity strays from that purpose, the harder it becomes to justify it as fair and reasonable.
		• The primary and secondary purpose distinction is less important than before.
			• It may be hard to work out what is fair and reasonable.
			• **No single factor** will determine whether a use is fair and reasonable and the **test will change** to reflect **evolving technology**.
			• The OAIC will provide guidance and practical examples to help organisations but the timing is problematic - we can't assess without guidance.
			• It is unclear how **genuine choice** will be approached. The Paper makes conflicting statements:
			  ○ "*choice will not be genuine where individuals are presented with 'take it or leave it' terms*" and
			  ○ "*the absence of choice does not necessarily mean that information handling is not fair and reasonable*'"

Consent needed to 'trade' information	• An organisation must not '**trade'** PI without consent.
	• There are 2 **exceptions**:
	  ○ Information 'strictly necessary' for a good/service (never available for marketing);
	  ○ Information from publicly available docs (even behind paywalls). Includes social media posts.
		• 'Trading' captures **direct marketing**.
		• It covers a broad range of arrangements where PI is disclosed as part of an exchange – e.g. **share transfer, exchange of customer lists**, any other exchange of PI for value (not just money).
		• It captures the disclosure of PI for uses that support or inform direct marketing, e.g**. cookies and pixels in programmatic advertising.**
			• This could impact significantly on programmatic advertising and may trigger more consent requests.
			• The extent to which data gathered at scale is excluded from the definition of PI will affect how broadly 'trading' is interpreted.
			• Even where entities rely on the publicly available doc exemption, the 'fair and reasonable' test will

Issue	Proposal	Practical impact	What remains unclear

		• 'Trading' does **not capture** the disclosure of data:
		  ○ where is it necessary to provide a product/service requested by the individual;
		  ○ where it is disclosed to a processor acting on behalf of a controller organisation (see below).
			still apply. This means scraping public information may not be fair game.

Consent needed to collect sensitive information	• An organisation must not collect sensitive information without consent.
	• There are 2 exceptions:
	  ○ Information 'strictly necessary' for a good/service (never available for marketing);
	  ○ Information from publicly available docs (even behind paywalls/registered accounts). Includes social media posts.
		• See above re definition of sensitive information.	• See above.

Notification	• Collection notice requirements will be simplified, removing much of the current overlap with privacy policies. • Notices will need to cover only **the fact and circumstances of collection** and **the intended purposes** of use/disclosure. • Notices must also be **clear and concise**.	• This change is likely to produce shorter, more accessible notices centred on purpose. • May see an increase in cookie-consent pop-ups.	• It is unclear whether the notice must be contemporaneous (e.g. cookie-consent pop ups).
Direct marketing	• APP7 would be replaced with a new**, technology neutral**, direct marketing framework. • 'Direct marketing' will cover marketing directed at an individual identified or targeted (individually or as part of a group) using personal information. • There is a core requirement to provide a **simple opt-out**, explained in **every communication**. • **Ad-supported services** (those earning revenue from making direct marketing communications,	• Includes **emails, SMS, targeted social media advertising, online behavioural advertising** based on PI, including **browsing history**. • This reflects the use of **profiling and audience segmentation.** • It clarifies that direct marketing includes **group-level targeting that relies on personal information.** • Each direct marketing communication would need to **include information on how an**	• Unclear is whether **content/product recommendations** (e.g. streaming or shopping sites) are caught. • The **ad-supported service** provisions may be tricky to apply given **uncertainty about what constitutes 'genuine choice'** — relevant factors flagged include how easy alternatives are to choose, the information given to explain them, and their comparative value.

Issue	Proposal	Practical impact	What remains unclear
	rather than from the goods/services advertised) may offer different terms to users who opt out, provided they retain a '**genuine choice**' to keep using the service without receiving marketing.	**individual may opt out** of direct marketing communications. • 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). • **Ad-supported services** are not required to continue to provide the same service to individuals who opt out. Instead, they can offer the service on different terms, provided those terms give the individual a **genuine choice** to continue using the service	• Seems to assume a broad definition of PI to cover **at scale inferences** – 'group level targeting'.

Data access and erasure (Schedule 4)

Issue	Proposal	Practical impact	What remains unclear?
Data access exceptions	• A new exception would let entities **decline access requests** where giving access remains unreasonable or impracticable due to **technical impossibility or infeasibility**.	• This should reduce burdens from broad access requests. • The exception won't apply where an entity has deliberately designed systems to frustrate access.	

Data erasure rights (applicable to 'large digital platforms')	• A new APP 14 would give individuals a right to request erasure of personal information held by 'large digital platforms':
	  ○ those with **at least $500 million in annual gross revenue**; and/or
	  ○ **at least 2.5 million average monthly Australian users**.
	• Platforms must comply within a **reasonable period** unless an exception applies (e.g. frivolous/vexatious requests, technical impossibility/infeasibility, or
		• **The relatively low thresholds may capture many organisations with an online presence even if they are not traditional 'digital platforms'**.
		• The types of digital services covered are broad (including any website).
		• The threshold of 2.5million average monthly users is likely to be met by many services, including those with limited revenue.
			• Analysis needed on what services will be caught by this definition.

Issue	Proposal	Practical impact	What remains unclear?
	information strictly necessary to keep providing a requested good or service).		

Exceptions for information processors (Schedule 6)

Issue	Proposal	Practical impact	What remains unclear?
Processors and controllers	• An APP entity is a 'processor' where it acts on behalf of a 'controller'. • The processor must act **under the controller's written instruction**s and for a **purpose the controller specifies in those instructions**. • A **processor acting on behalf of a controller will not be liable under the APPS** (except APP 1 (privacy policy) and APP11 (security)).	• The distinction only applies where both entities are bound by the APPs. • The Act doesn't cover small businesses, so a processor servicing a small business controller may still carry the full weight of APP obligations, unlike when servicing a larger customer. • The exception only applies where the processor acts within the controller's written instructions**. The way in which instructions are scoped and documented will be key**. • This will lead to more formal documentation than is currently the case. Instructions can still leave technical/operational detail to the processor's discretion.	• This may become a problem in commercial negotiations, with controllers and processors each keen to minimise their own risk.