

# Privacy reset on a deadline

## Key changes and practical steps for businesses

Australia – September 2026

In a record 1.5 months from the attorney-general's announcement that her office would "[consult] on a second tranche of privacy reform to responsibly strengthen, modernise and simplify Australia's personal data protection laws", the Australian government has delivered, with an exposure draft of the *Privacy Amendment (Personal Data Protection) Bill 2026 (Cth)* (Draft Bill) released on 21 August.

The Draft Bill arrives with a consultation paper (Paper), which clarifies how some of the proposals in the Draft Bill could operate while seeking feedback on other proposed measures under development. In particular, the Paper focuses on recent areas of public attention, asking whether additional measures are required to regulate new technologies such as wearables.

The Draft Bill is subject to consultation until 18 September, with responses limited to 1,000 words. This suggests that, after years of consulting on privacy reform, the government has crafted the Draft Bill to minimise challenge and put forward ready-to-go amendments that they think reflect consensus (or something close to it). This is supported by the introduction to the Draft Bill, which emphasises that most of the proposals have been taken from the government response to the Privacy Act Review Report (Government Response).

We have summarised highlights from the Draft Bill below, as well as what these might mean in practice and questions or concerns that we have. While the Paper also asks stakeholders whether the proposals adequately protect the privacy risks associated with emerging technologies, our sense of both the Draft Bill and the attorney-general's accompanying announcement is that the *Privacy Act 1988 (Cth)* (Privacy Act) will continue to regulate these devices in general and from a tech-neutral perspective, with no discrete and specific focus on any one kind of technology (regardless of the public attention).

The Draft Bill notably excludes most of the proposals in the Government Response, including tinkering with the small business and employee record exemptions or granting individuals a direct right of action. It is difficult to predict whether these will reenter the conversation in the future, but, for now, we expect that the Draft Bill reflects the furthest that the government is willing to go.

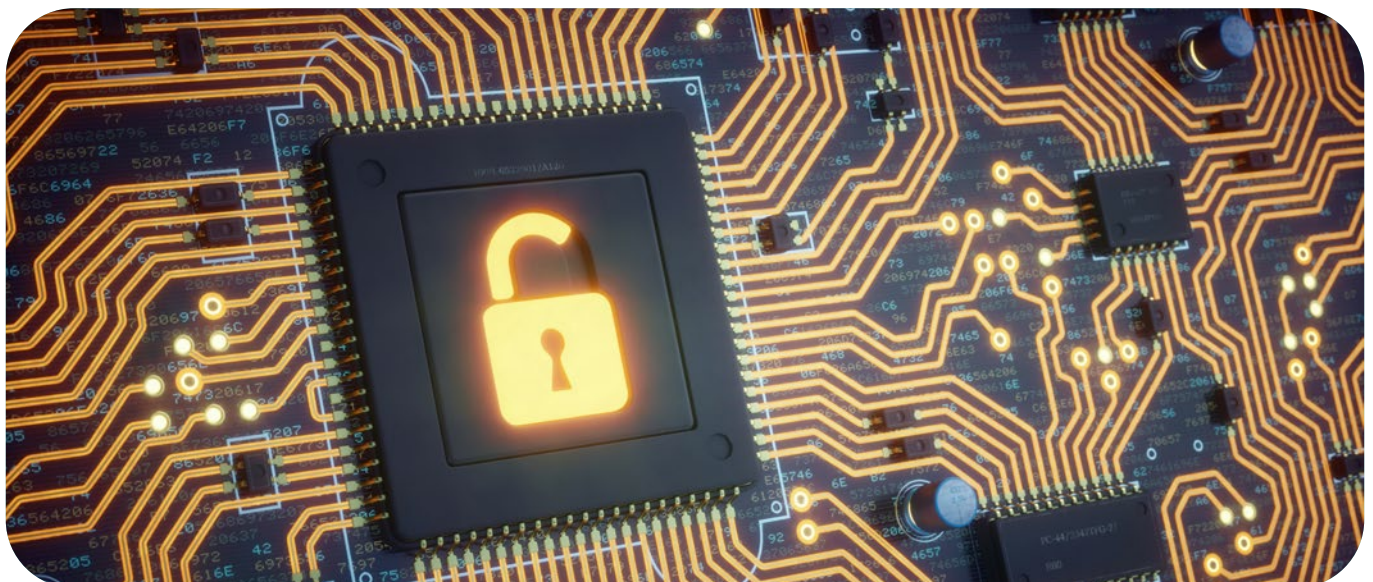


## Overarching changes

| Change                                                                                       | Effect                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Primary impact                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Related impacts                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Revised definition of "personal information" and new definition of "reasonably identifiable" | <p>The definition of "personal information" will expressly include information or an opinion "that relates to" (rather than is "about") an individual or information from which an individual that is reasonably identifiable.</p> <p>"Reasonably identifiable" is defined for the first time, to mean information that is identifiable by being combined with other reasonably available information or opinions.</p>                                                                                                                                                                                                                                                                                                                                                                           | <p>This change reflects the Office of the Australian Information Commissioner's (OAIC) recent decisions, which broke away from previous findings by establishing that "personal information" would include information that facilitates "individuation": that is, the singling out or distinguishing of an individual from others (even if personal identifiers like name remain unknown) in a way that affects their rights and interests.</p> <p>This is consistent with the Paper, which includes as a criterion for the "relates to" test whether information "says something" about an individual's behaviour or activities or if it is used to inform or influence actions or decisions that affect the individual.</p> <p>To the extent that this was not already the case, "personal information" will extend to inferences, opinions and other information (e.g. information generated by AI technologies) that relates to an individual.</p> | <p>Under the Draft Bill, "direct marketing" will be defined to include marketing to an individual who is targeted either individually "or as a member of a class", but the changes to these definitions also expand the application of the term (as well as any other Australian Privacy Principle (APP) that applies to "personal information").</p>                                                                                                                                                                                                                                                                                                                                                                |
| Fair and reasonable test                                                                     | <p>This is the hallmark of the Draft Bill. Rather than requiring the collection, use and disclosure of personal information meet the highly specific requirements of APPs 3, 4 and 6, these have been repealed, with a new requirement that an APP entity only collect, use or disclose personal information where the collection, use or disclosure is fair and reasonable (and lawful) in the circumstances.</p> <p>"Fair and reasonable" requires APP entities to have regard to (but not necessarily satisfy all of) six legislated factors, including an individual's reasonable expectations of privacy, the APP entity's transparency about its information handling and whether the relevant purpose could be achieved through handling less information or nonpersonal information.</p> | <p>The "fair and reasonable" test has been foreshadowed for months, but many will be pleased to see that the government intends the test to operate <i>in lieu of</i> additional requirements in APPs 3, 4 and 6, avoiding both overregulation and overreliance on measures with which consumers rarely engage (e.g. consent under APP 6.1(a)). In this way, the government has partially taken heed of the Productivity Commission's recommendation that an outcomes-based privacy duty should replace certain existing controls-based requirements.</p> <p>However, "fair and reasonable" presents certain practical challenges. For one, it is clear from the Paper that transparency – a mandatory consideration under new APP 3.2(b) – is not enough to establish "reasonable" expectations, although the total absence of transparency would kill any such argument.</p>                                                                         | <p>This will affect everything (including because it operates on a retrospective basis, to personal information already collected) but impacts that immediately come to mind include:</p> <ul style="list-style-type: none"> <li>• No more requirement (previously in APP 3.6) that APP entities should generally only collect personal information directly from an individual, provided that in collecting such personal information, the "fair and reasonable" test is always met.</li> <li>• The requirement in APP 11 to delete or destroy personal information once no longer necessary has met its corollary in new APP 3.2(c), which requires data minimisation to be considered from the outset.</li> </ul> |

| Change                      | Effect                                                                                                                                                                                                                                               | Primary impact                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Related impacts                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                             |                                                                                                                                                                                                                                                      | <p>For another, the test seems to discourage organisations from novel uses of personal information, as it will be more difficult to establish that an individual is aware of, and has genuine choice over, such uses. Finally, the use of “reasonable”, both in new APP 3.1(a) and throughout the Draft Bill, is intended to give organisations flexibility but could create uncertainty as different organisations debate how to assess reasonableness across a broader user base.</p> <p>While “fair and reasonable” has been compared to “legitimate interests” under the GDPR, “legitimate interests” is crafted as a permission, while it is clear from the Paper that “fair and reasonable” operates as a condition.</p> | <ul style="list-style-type: none"> <li>Existing permissions to use personal information for a secondary purpose where supported by consent or if the secondary purpose is “reasonably related” have fallen away, in favour of the “fair and reasonable” test. However, whether an individual has a “genuine choice” as to the collection, use or disclosure of their personal information, or whether it is within their reasonable expectations, remains relevant: see APP 3.2(a) and (e).</li> </ul> |
| New definition of “consent” | <p>“Consent” has been redefined so that it must be:</p> <ul style="list-style-type: none"> <li>Voluntary</li> <li>Informed</li> <li>Current</li> <li>Specific</li> <li>Unambiguous</li> </ul> <p>regardless of whether it is express or implied.</p> | <p>This definition is consistent with the OAIC’s guidance,<sup>1</sup> as well as the use of consent in other legislation, including Part 4A of the <i>Online Safety Act 2023</i> (Cth).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <p>Entities will need to refresh any consents on which they seek to rely, at least in the context of the Privacy Act. At least initially, the Spam Act appears to be unaffected, but that may change (as was the case for the GDPR and the ePrivacy Directive).</p> <p>Alongside its removal of APPs 3 and 6, it is clear that the government’s intention here is to minimise reliance on consent where this is not a meaningful option for individuals.</p>                                           |

1 OAIC, “[Consent to the handling of personal information](#)”.



## Sensitive information

| Change                                                           | Effect                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Primary impact                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Related impact                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Revised definition of "sensitive information"                    | The definition of "sensitive information" will expressly include precise geolocation tracking data, which identifies an individual's specific location to within a radius of 500 metres and is collected and held by reference to their location over time.                                                                                                                                                                                                                | Consistently with other privacy laws (such as the UK <i>Privacy and Electronic Communications Regulations</i> 2003 (PECR)), APP entities will need to seek consent before collecting precise geolocation tracking data.                                                                                                                                                                                                                                                                                                                                                                                                | Consent to location tracking often already takes place as a matter of good practice, including through iOS- and Android-enabled app permissions. It will be interesting to see if app stores contractually require developers to independently obtain consent or expand their offering of existing permission features.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| New exemptions from collecting consent for sensitive information | <p>An APP entity will not require consent when collecting sensitive information from a publicly available document or where such collection is "strictly necessary" to deliver goods or services requested by an individual. However, the "fair and reasonable" test will continue to apply.</p> <p>An APP entity will not have collected sensitive information only because the entity collects personal information from which sensitive information can be derived.</p> | While the definition of "sensitive information" has expanded (see above), so too have the permissions to use such information. In addition, the government seems to have shifted away from the OAIC's view that, in certain circumstances, mere possession of sensitive information (e.g. an individual's visit to a website providing counselling services <sup>2</sup> or an image where an individual's ethnic origin is apparent <sup>3</sup> ) would, without anything further, constitute sensitive information. This is a helpful clarification for business, who would have found such a condition unworkable. | <p>In our view, the government's clarification could theoretically change the impact (if not the outcome) of recent OAIC decisions. For example, it is at least arguable that where Medmate collected a user's browsing data,<sup>4</sup> this data would only become sensitive information if Medmate were using or disclosing this information as sensitive information (rather than it automatically falling within this category).</p> <p>Interestingly, this is not the first time that we have seen "strictly necessary" in a privacy-related legislative instrument. The draft Children's Online Privacy Code requires an entity's collection, use or disclosure of personal information about a child to be "strictly necessary" to provide a service.<sup>5</sup> It remains to be seen what this term adds to the concept of "necessary" (as opposed to "reasonably necessary", where the distinction is clear).</p> |

<sup>2</sup> OAIC, "[Tracking pixels and privacy obligations](#)" (4 November 2024).

<sup>3</sup> OAIC, "[Posting photos and videos](#)" (13 June 2019).

<sup>4</sup> *Commissioner Initiated Investigation into Medmate Australia Pty Ltd (Privacy)* [2026] AICmr 41.

<sup>5</sup> Section 9, *Privacy (Children's Online Privacy) Code* 2026 (Cth).

## Third party information handling

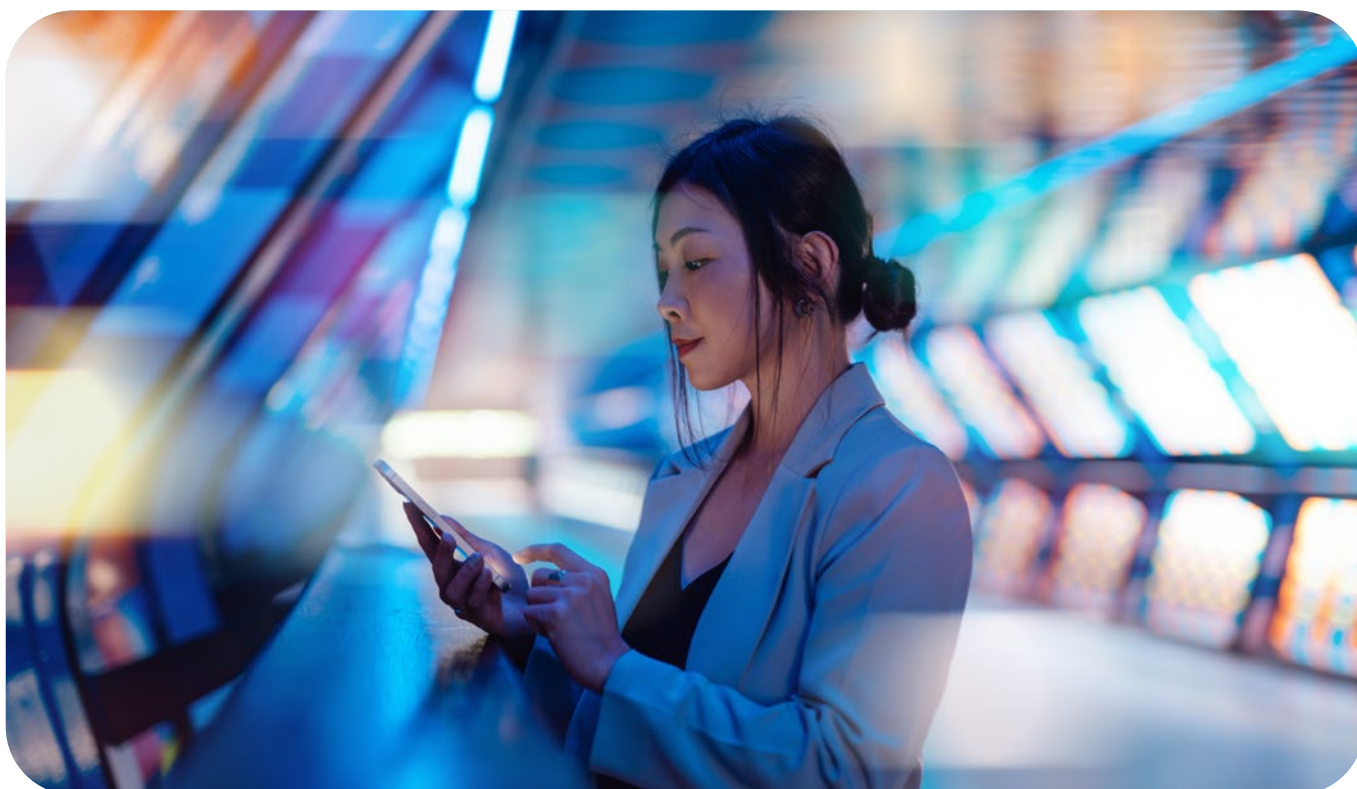
| Change                                       | Effect                                                                                                                                                                                                                                                    | Primary impact                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Related impact                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Limited concepts of controller and processor | Where a processor does an act or engages in a practice on behalf of a controller and in accordance with that controller's written instructions, then the controller (and not the processor) shall be liable where that act or practice breaches the APPs. | <p>This change brings the Privacy Act closer into line with international practice, where most developed countries distinguish between controllers and processors who act on their instructions and on their behalf. It is also consistent with the OAIC's updated guidance on APP 3,<sup>6</sup> which recognises that an entity may have "control" over personal information (even if it does not have possession).</p> <p>The same guidance emphasises the necessity of having in place a contract that covers how personal information will be handled, and each party's obligations under the Privacy Act. This is reiterated in the Paper, which recommends clear and documented instructions between controllers and their processors.</p> | <p>Unlike Article 28 of the GDPR, the Draft Bill does not expressly reference contracts, and the Paper suggests that there "is no prescribed format or template" for a controller's instructions. However, this seems like the most logical means of ensuring that instructions are adequately documented (including previously informal instructions).</p> <p>As is the case now, processors will face difficulty where an exemption (like employee records or small business) means that controllers are not directly responsible for complying with the APPs, shifting liability onto processors. The converse will also apply, where controllers find that their "small business" suppliers are not caught by the Privacy Act.</p> <p>Processors will also face difficulty in circumstances where responsibility for compliance is shared, specifically, under APP 11, which the Draft Bill recognises may still impose direct responsibility on processors. Without further clarity from the government or the publication of standard contractual clauses, we anticipate significant negotiation between controllers and processors in these areas, especially if they are large and sophisticated suppliers. It is also possible that even though liability sits with the controller under the law, the controller will make sure that this is "back-to-backed" by its contractual liability arrangements with the processor.</p> |

<sup>6</sup> OAIC, "[Australian Privacy Principles Guidelines – Chapter 3: APP 3 Collection of solicited personal information](#)".



| Change                   | Effect                                                                                                                        | Primary impact                                                                                                                                   | Related impact                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                          |                                                                                                                               |                                                                                                                                                  | Interestingly, the government has not referenced the possibility of joint or separate controllers – many entities (especially in the programmatic advertising world) will want to ensure that their contracts cover liability in relationships that go beyond the traditional controller/process distinction.                                                                                                                                                                                                                                                             |
| Definition of “disclose” | “Disclose” is defined for the first time, to mean an entity making personal information accessible to another person or body. | This is a welcome development, as it clarifies the distinction between “use” and “disclosure” (which the OAIC has always informally recognised). | Typically, APP entities have avoided restrictions on disclosure when providing personal information to an overseas contractor (such as a cloud service provider) to perform services on their behalf, provided that they have not released the handling of personal information from their effective control. <sup>7</sup> Given the new definition, it is unlikely that this exception will continue to apply, although the contractor will not be liable for acts or practices performed on behalf of the controller, and within the controller’s written instructions. |

7 OAIC, “[Australian Privacy Principles Guidelines – Chapter 8: APP 8 Cross-border disclosures of personal information](#)”.



## Direct marketing

| Change                           | Effect                                                                                                                                                                                                                                                                                                | Primary impact                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Related impact                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Definition of "direct marketing" | "Direct marketing" now expressly extends to any form of communication of advertising or marketing material to an individual, including if they are targeted (either as an individual or as member of a class) and if the targeting is done using personal information that relates to the individual. | <p>The government has resolved the ongoing debate, continued in the Government Response, as to whether direct marketing covers targeted advertising. The Paper aligns with OAIC guidance,<sup>8</sup> noting that any "email, text message, telemarketing call, targeted social media advertising and online behavioural advertising" could fall within the definition. However, we query whether the updated definition would cover marketing to a member of a class where the criteria for selecting that member (or the class more broadly) involves deidentified or nonpersonal information, and whether it would extend to marketing material created by individuals and communicated through nontraditional means (e.g. through social media content).</p> <p>The Privacy Review floated the possibility of requiring consent to targeted advertising. Thankfully, the Draft Bill has not waded so far in, but the threshold for proving that direct marketing is "fair and reasonable" is likely to be higher than for other activities.</p> | <p>The expansion of "direct marketing" means that while an APP entity must offer an opt-out to individuals, the Draft Bill requires only that it takes "reasonable steps" to action such opt-out, recognising that in practice, linking an individual to different accounts, devices and identifiers may be difficult. While the responsibility for opt-outs has typically fallen on advertisers, the Consultation Paper suggests that it will now sit with the organisation who directly makes the communication (such as a social media platform). This is a change from current practice – clear contractual division of obligations will be critical.</p> <p>While the Draft Bill contemplates that entities may offer individuals only a partial opt-out of ad-supported services (provided that they offer individuals a "genuine choice"), this may be challenging to apply in practice. According to the Paper, the government has taken the "consent-or-pay" model in the EU as its inspiration for this approach, but the interpretation of this approach has differed. For example, the European Data Protection Board<sup>9</sup> considers that, in most cases, large online platforms will struggle to demonstrate valid consent where users face only a binary choice between a free service (with behavioural advertising) or a paid service.</p> |

<sup>8</sup> OAIC, "[Direct marketing](#)" (1 May 2019).

<sup>9</sup> European Data Protection Board, [Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms](#) (17 April 2024).



| Change                                                         | Effect                                                                                                                                                                                                                                          | Primary impact                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Related impact                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Prohibition on trading on personal information without consent | Consent will be required for all “trading” in personal information. There are numerous exceptions, including normal controller-processor relationships and where such trading is incidental to the sale, acquisition or transfer of a business. | <p>Any relief that marketers felt when learning that direct marketing would not be subject to consent will fall away upon reading this restriction. “Trading” is defined broadly and could extend to pixel-based marketing, as well as more standard data brokerage. Our read is that it will cover any scenario where an entity buys or sells personal information to another entity (including feeding back results), including most forms of third party-facilitated marketing.</p> <p>Given the breadth of both “trading” and “direct marketing”, it is likely that advertisers will need to comply with both sets of requirements when, for example, engaging in programmatic advertising involving the use or disclosure of third party-sourced personal information. This would be a particularly onerous result.</p> | <p>Given the enhanced requirements for consent under section 6AAB of the Draft Bill (see <a href="#">[insert link]</a>), it is unlikely that a cookie consent (or similar) banner will be enough to constitute valid consent to trading. Unlike the collection of sensitive information, there is also no exemption where the personal information has been made publicly available.</p> <p>A disclosure is not a trade when personal information is disclosed to a processor acting on behalf of a controller and only in accordance with its documented instructions. However, it seems unlikely that most in the adtech ecosystem will want to accept that limited level of control.</p> |





## Data Security

| Change                          | Effect                                                                                                                                                                                                                                                                             | Primary impact                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Related impact                                                                                                                                                                                                            |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data breach notification        | APP entities must notify eligible data breaches to both the OAIC and individuals within 72 hours of becoming aware that there are reasonable grounds to suspect an eligible data breach. The notification must contain the information in section 26WK(3).                         | <p>This change will necessitate all APP entities to review and revise their breach notification and management policies and procedures. However, entities have retained a period in which to assess whether “reasonable grounds” for suspecting a data breach exist (generally, 30 days) – the 72-hour period only applies once that assessment has been made.</p> <p>Helpfully, the Draft Bill allows for phased notification, provided that an APP entity considers it impossible or impracticable to provide all of the information required and, as soon as practicable, rectifies this with updated written notice.</p> <p>In respect of notification to affected individuals, the Draft Bill follows a similar direction to Article 34(3) of the GDPR, allowing entities to avoid notification where remedial action is taken which means that the breach is not likely to result in serious harm. This, too, is a helpful exception, recognising that certain information security protections (like encryption) or other speedy action can help avoid wider knowledge of the breach.</p> | Controllers will want to make sure that any arrangements with processors (see <b>[insert reference]</b> ) cover off on the new notification period.                                                                       |
| Noneligible data breaches       | Even if it is not an eligible data breach, APP entities are still required to take reasonable steps to prevent or reduce harm to any individuals involved in an actual or suspected data breach.                                                                                   | This effectively legislates the kind of “best practice” data security and breach management practices that many organisations already have in place. To the extent that this is not already covered, APP entities should ensure that their processes pick up on noneligible, as well as eligible, data breaches, and require at least internal notification and mitigation where appropriate.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Controllers will want to make sure that any arrangements with processors (see <b>[insert reference]</b> ) cover off on the notification and mitigation of both minor and eligible data breaches.                          |
| Destruction or deidentification | <p>APP entities will be required to:</p> <ul style="list-style-type: none"> <li>Actively consider destroying information before taking the option of deidentification</li> <li>Regularly evaluate the effectiveness of measures taken to comply with APPs 11.1 and 11.2</li> </ul> | <p>There is no obligation for APP entities to destroy personal information if it has considered destruction but believes that deidentification is the appropriate option.</p> <p>Equally, on our reading, there is no obligation to actively assess whether information is still necessary for a lawful purpose under the APPs. Rather, new APP 11.5 requires that an APP entity assess the effectiveness of measures used to destroy or deidentify personal information.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Please see too the obligation for an APP entity to implement – as part of ensuring that their collection, use or disclosure is “fair and reasonable” – data minimisation from the outset: see <b>[insert reference]</b> . |

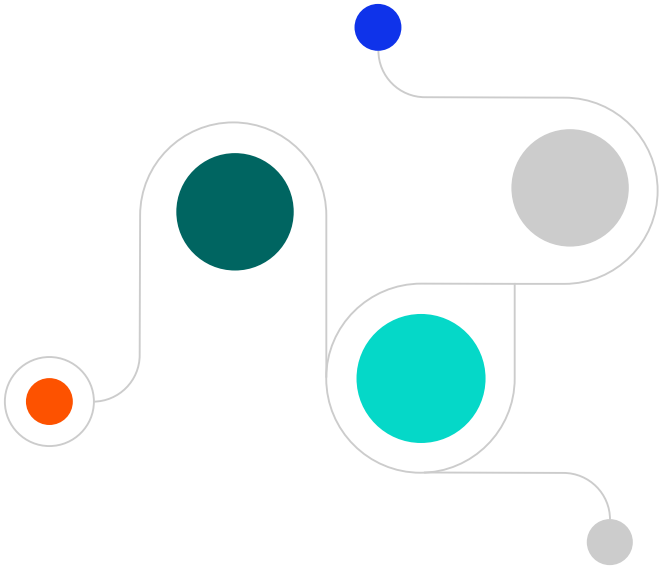
Individual rights

| Change           | Effect                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Primary impact                                                                                                                                                                                                                                                                  | Related impact                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Right to erasure | <p>New APP 14 requires only “large digital platforms” (i.e. a social media service, relevant electronic service or designated internet service, whose business group meets the gross revenue test of AU\$500 million or who has an average of 2.5 million monthly end users in the previous financial year) to destroy an individual’s personal information on request, unless an exception applies.</p> <p>Exceptions include:</p> <ul style="list-style-type: none"><li>• A request that is frivolous or vexatious</li><li>• A request in respect of a permitted general or permitted health situation</li><li>• Where an organisation is required to retain the personal information under law</li><li>• A request that is technically impossible or infeasible</li><li>• Where the personal information is strictly necessary to provide or deliver goods or services.</li></ul> | <p>This is a significant change to current practice, although it is good to see that the exceptions are broader than what was contemplated in the Government Response (including the references to permitted general and health situations, some of which are quite broad).</p> | <p>It is unclear as to why the right to erasure has been limited to large digital platforms, especially when the OAIC’s latest Notifiable Data Breaches Report<sup>10</sup> revealed that most data breaches have been suffered by financial services providers and Australian government agencies. In combination with the right to erasure, which the draft Children’s Online Privacy Code proposes to grant to children alone, this risks further fragmentation of individual rights, and confusion amongst individuals as to which rights apply and when.</p> |

Author



**Tanvi Mehta Krensel**  
Partner, Sydney  
T +61 450 657 742  
tanvi.mehtakrensel@squirepb.com



10 OAIC, “[Data breach notifications increase to all-time high in 2025, new NDB stats show](#)” (6 July 2026).