MinterEllison.

Tranche 2 Privacy Act reforms

Table of amendments — how the exposure draft changes the current position

AREA OF REFORM	CURRENT PRIVACY ACT POSITION	PROPOSED AMENDED POSITION	HIGH-LEVEL COMMENTARY
Definition of 'personal information'	Information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not.	Information or an opinion that relates to an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not. With added clarification that an individual can be identified or reasonably identified even if information allows an individual to be 'recognised, singled out, or otherwise dealt with as a distinct individual in practice'. Note: this definition incorporates the new proposed definition of 'reasonably identifiable'.	The proposed amended position broadens the definition of 'personal information' to capture a wider array of information.
Definition of 'reasonably identifiable'	The Privacy Act does not currently provide a definition for this term.	An individual is reasonably identifiable from information or an opinion if the individual could be identified by combining the information or opinion with other information or opinions that are readily available.	This proposed definition may broaden the range of information captured as 'personal information', given the volume of information that may be 'readily available' across emerging technologies. It may also be more difficult for organisations to argue information has been properly 'de-identified'.
Definition of 'de-identified'	Personal information is de-identified if the information is no longer about an identifiable individual or an individual who is reasonably identifiable.	Information or an opinion is de-identified at a particular time, or in particular circumstances, if, at that time or in those circumstances, the information or opinion has ceased to be information or an opinion that relates to an identifiable individual or an individual who is reasonably identifiable. Note: this definition incorporates the new proposed definition of 'reasonably identifiable' above.	This may make it more difficult for organisations to properly de-identify information, given the broad definition of when an individual may be 'reasonably identifiable'.
Collection of solicited personal information	APP 3 requires that APP entities only collect solicited personal information where it is reasonably necessary for (and, in the case of agencies, directly related to) the organisation's functions or activities, and only where collection is undertaken by lawful and fair means.	An APP entity may only collect personal information if that collection is 'fair and reasonable in the circumstances' and is lawful.	This represents a significant change in the legislative test for collection of personal information.
Collection of unsolicited personal information	APP 4 requires that APP entities destroy or de-identify unsolicited personal information which is not reasonably necessary for an organisation's functions or activities.	An APP entity may only collect personal information if that collection is 'fair and reasonable in the circumstances' and is lawful.	This represents a significant change in the legislative test for the handling of unsolicited personal information.
Use and disclosure of personal information	APP 6 provides that APP entities may use or disclose personal information for the purpose for which it was collected, unless an exception applies.	An APP entity may only use or disclose personal information if that use or disclosure is 'fair and reasonable in the circumstances' and is lawful.	This represents a significant change in the legislative test for the use and disclosure of personal information.
Controller and processor	The concepts of 'controller' and 'processor' are not found in the current Privacy Act.	New concepts of 'controller' and 'processor' would be introduced and apply such that APP breaches by the processor would be taken to be breaches of the controller.	These concepts align with the European Union General Data Protection Regulation (GDPR) and UK GDPR. APP entities engaging third party contractors who are also APP entities may incur liability for privacy breaches performed under their direction.
Data breach	'Data breach' is not a defined term in the current Privacy Act.	The Bill proposes the following definition (relevantly for APP entities). If: (a) there is unauthorised access to, or unauthorised disclosure of, the information; or (b) the information is lost in circumstances where there is likely to be unauthorised access to or disclosure of the information; the access, disclosure or loss is a data breach of the APP entity.	APP entities would have new obligations to respond to data breaches effectively and mitigate the potential impacts on individuals.
Eligible data breach	An eligible data breach occurs if: (a) both of the following conditions are satisfied: (i) there is unauthorised access to, or unauthorised disclosure of, the information; (ii) a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates; or (b) the information is lost in circumstances where: (i) unauthorised access to, or unauthorised disclosure of, the information is likely to occur; and (ii) assuming that unauthorised access to, or unauthorised disclosure of, the information were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates. An APP entity must notify the regulator as soon as practicable after the entity becomes aware there are reasonable grounds to believe an eligible data breach has occurred.	An eligible data breach occurs if: (a) for a data breach constituted by unauthorised access to, or disclosure of, information — a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates; or (b) for a data breach constituted by a loss of information — a reasonable person would conclude that any unauthorised access to, or unauthorised disclosure of, the information would be likely to result in serious harm to any of the individuals to whom the information relates. An APP entity must notify the regulator within 72 hours after the entity becomes aware there are reasonable grounds to believe an eligible data breach has occurred.	The amended definition of 'eligible data breach' would require businesses to review their data breach response plans and ensure eligible data breaches are notified within the 72-hour timeframe.
Security of personal information	APP 11 currently requires that an APP entity takes reasonable steps to destroy or de-identify personal information it no longer needs for any purpose for which the information may be used or disclosed under the APPs.	The Bill proposes a new obligation that an APP entity must be able to identify the personal information that can be destroyed or de-identified, and undertake regular assessments of its ability to comply with the new APP 11 requirements.	This would impose new responsibilities on APP entities to ensure appropriate data governance processes are in place.
Consent	'Consent' is not currently defined in the Privacy Act. However, Office of the Australian Information Commissioner (OAIC) guidance provides that consent can be explicit or implied, and must be informed, voluntary, current, and specific.	For the purposes of this Act, an individual's consent may be express or implied, but must be all of the following: (a) voluntary; (b) informed; (c) current; (d) specific; and (e) unambiguous.	This provides clarification on consent requirements.
Trading personal information	The current Privacy Act does not define what it means to 'trade' personal information.	To trade personal information means where disclosure is made: (a) for money or other consideration; or (b) for the purposes of direct marketing. Unless an exception applies, APP entities must not trade personal information without the individual's consent.	This would be a new obligation.
Direct marketing	APP 7 provides that an APP entity must provide a 'simple means by which the individual may easily request not to receive direct marketing communications from the organisation'.	APP entities would also be required to provide information to individuals that sets out how they may request not to receive direct marketing communications from the organisation, and such information must be: (a) set out in clear and plain language; (b) readily understandable by an ordinary person; (c) up-to-date; and (d) concise.	This would be a new obligation.
Right of erasure	The APPs currently provide a right for individuals to access or request a correction of their personal information held by an APP entity, but there is no current right of erasure.	Large digital platforms which meet proposed legislative criteria would be required to destroy personal information they hold about a person upon request from that individual, unless an exception applies.	This would be a new obligation imposed on APP entities that qualify as large digital platforms.
Human research exception	Currently, entities undertaking human research are required to satisfy a research exception under the Privacy Act and obtain ethics approval.	One research exception would be set out in the Privacy Act. The Privacy Commissioner (following further consultation) would issue one set of privacy guidelines.	This would likely constitute a significant overhaul of current privacy pathways for research.
Collection statement requirements	APP 5 currently requires APP entities to notify individuals of specific matters when collecting their personal information.	The Bill proposes to further clarify this obligation by requiring that notices must be: (a) in clear and plain language; (b) readily understandable by the individual; (c) up-to-date; and (d) concise.	This provides clarification on existing notice obligations.