KPMG

Privacy Act Review Report

KPMG submission

KPMG Australia, April 2023

KPMG.com.au

Contents

Executive summary

As a leading professional services firm, KPMG Australia (KPMG) is committed to meeting the requirements of all our stakeholders – not only the organisations we audit and advise, but also employees, governments, regulators – and the wider community. We strive to contribute in a positive way to the debate that is shaping the Australian economy and we welcome the opportunity to provide a submission in response to the proposals in the Attorney-General's Department Privacy Act Review Report (the report).

KPMG has been actively involved in the Review of the Privacy Act (the review), providing submissions in response to both the Issues Paper[1] and Discussion Paper.[2] As we have previously outlined, entities must currently manage and comply with a range of data-related regulatory frameworks. Reforms to the Privacy Act need to carefully consider the broader landscape of data-related regulatory requirements that exist in overlapping and, in some cases, fragmented frameworks at both a state and federal level and how changes will interact with evolving cyber security regulations as a result of the Cyber Security Strategy which is also currently undergoing a consultation process.

To assist with the above, KPMG welcomes the proposal to review all legal provisions that require the retention of personal information and the further clarification regarding the extraterritorial operation of the Privacy Act in light of the amendments made by the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 (Privacy Enforcement Bill). KPMG notes that many of the proposals align the Australian Privacy Act 1988 (Act) with the General Data Protection Regulation (GDPR) and other harmonisation efforts globally, which will help with complexity in complying with regulations when businesses operate across borders.

Given the scale of the changes proposed, it will be important to support businesses through the implementation of the proposals that are adopted. Two key approaches to consider could be first to adopt a tiered and prioritised approach to introducing the reforms and second, to set out staged compliance dates to enable entities to prepare for further changes that may be adopted.

KPMG considers that a critical aspect of reforming the Privacy Act should be provisioning for an appropriately resourced regulator so that it can achieve the right balance of enforcement, oversight, guidance and support. KPMG supports enforcement powers similar to like regulatory bodies – ones that can be exercised in the context of the right privacy settings and are designed to promote compliance and provide clarity.

KPMG has previously outlined the importance of code-making as a key regulatory tool in the regime, as Australian Privacy Principles (APP) code-making powers are a preferred method of addressing discrete issues in the Act. We consider that further clarity about the process required for code-making is required and recommend outlining a clear framework similar to those of ASIC's Management Accountability Regime or the Online Privacy Code to ensure any codes are carefully developed.

Thank you for the opportunity to participate in the consultation process and we look forward to working with the government on implementing reform to the Privacy Act. If you would like to discuss the contents of this submission further, please do not hesitate to reach out.

Yours sincerely,

Veronica Scott
Partner, Cyber and Privacy Law
KPMG Australia

Kelly Henney
Partner, Privacy and Data Protection
KPMG Australia

[1] https://kpmg.com/au/en/home/insights/2021/01/review-privacy-act-1988-cth-kpmg-issues-paper.html
[2] https://kpmg.com/au/en/home/insights/2022/01/review-privacy-act-1988-kpmg-submission.html

Background

About KPMG

KPMG is a global organisation of independent professional firms, providing a full range of services to organisations across a wide range of industries, governments and not-for-profit sectors. We operate in 146 countries and territories and have more than 227,000 people working in member firms, including law firms, around the world. In Australia, KPMG has a long tradition of professionalism and integrity combined with our dynamic approach to advising clients in a digital-driven world.

KPMG acknowledges its contribution to the reform agenda benefits from a diversity of skills and experience. We have brought together a broad team of specialists across our risk, technology, law, cyber security, regulatory, compliance, ethics and strategy offerings to provide a comprehensive response to a complex area of law.

Section 1:
KPMG recommendations

RECOMMENDATION 1:

KPMG recommends that given the scale of the changes proposed, the implementation of proposals that are adopted should be done in a tiered and prioritised approach. Further, the implementation of any proposals where further clarity and/or consultation is required, or which have a major impact on compliance obligations will require additional time.

RECOMMENDATION 2:

KPMG recommends that reforms to the Privacy Act should carefully consider the broader landscape of data and cyber-related regulatory requirements. These exist in overlapping and, in some cases, fragmented frameworks at a state and federal level, and KPMG welcomes ongoing reviews into harmonising the requirements.

RECOMMENDATION 3:

KPMG considers that an appropriately resourced regulator is a critical aspect of these reforms. The Office of the Australian Information Commissioner (OAIC) should have adequate resources to ensure they can achieve the right balance of enforcement, oversight, guidance and support. KPMG supports enforcement powers similar to like regulatory bodies that can be exercised in the right privacy settings that promote compliance and provide clarity.

RECOMMENDATION 4:

KPMG supports preserving the current definition of personal information. However, if it is amended to change the word ‘about’ to ‘relates to’, KPMG recommends further consultation with industry and engagement with the Commonwealth Scientific and Industrial Research Organisation (CSIRO) in relation to the concept of de-identified and pseudo-anonymised data.

RECOMMENDATION 5:

KPMG considers that further clarity about the concept of ‘de-identified’ information is required and it may be better governed under industry-specific codes rather than being inserted into and expressly regulated by the Act. In any event, this should be the subject of further guidance which also allows flexibility to evolve.

RECOMMENDATION 6:

Given the complexity of genomic information, KPMG recommends that specific rules, provisions, and exemptions be considered and made clear in the Act, and that guidance be provided in relation to the use of genomic information.

RECOMMENDATION 7:

KPMG recommends that steps to remove the small business exemption must be undertaken in a well-planned and consultative manner, and be subject to a comprehensive Regulatory Impact Statement that includes consideration with how the proposed changes interact with other aspects of the current regulatory framework, including proposed changes to cyber security regulations as a result of the Cyber Security Strategy. While changes to this exemption can help uplift broader compliance in the supply chain, it will have a significant impact and impose additional regulation. It may be beneficial to consider a phased approach that begins with higher-risk small business.

RECOMMENDATION 8:

KPMG suggests refinements to APP 12, to copy some of the exceptions/provisions of the Freedom of Information Act, in terms of the ability to decline access requests from individuals if meeting those

requests will unduly divert resources. Instead, we propose requiring individuals to refine the scope of their access/correction requests.

RECOMMENDATION 9:

KPMG supports the introduction of new definitions in relation to direct marketing, however recommends that care must be taken to avoid inadvertently capturing certain activities while still being broad enough to capture emerging technologies. For example:

- "targeting" should not be so broad as to capture activities that are not intended to be targeted to a known individual; and
- "trading" should not be so broad as to cover processing activities performed by a processor for a data controller or the sale of a business such as by shares/assets.

RECOMMENDATION 10:

KPMG supports the proactive approach to improved privacy protections for all people experiencing vulnerability and welcomes non-exhaustive guidance on factors that indicate when an individual may be experiencing vulnerability as it will not necessarily be a persistent state.

RECOMMENDATION 11:

KPMG welcomes the proposal for the Commonwealth to review all legal provisions that require the retention of personal information.

RECOMMENDATION 12:

KPMG supports the addition of retention periods for which the information will be stored into privacy notices and policy.

RECOMMENDATION 13:

KPMG considers that there may be a role for a 'best practice' remediation template to be developed in consultation with industry.

Section 2:
KPMG insights

List of proposals

PROPOSAL	KPMG RESPONSE
2. Objects of the Act	
Proposal 3.1 Amend the objects of the Act to clarify that the Act is about the protection of personal information.	KPMG supports this proposal which clarifies that the Act's scope relates specifically to information privacy.
Proposal 3.2 Amend the objects of the Act to recognise the public interest in protecting privacy.	While KPMG agrees there is a public interest in protecting privacy, this needs to also be balanced with other public interests and rights. KPMG therefore considers that amending the objects of the Act to recognise the public interest may require further consideration in order to avoid unduly narrowing an entity's legitimate purposes and objectives and to recognise that these may serve other public interests. Public interest could instead be a separate basis for lawful processing, including in relation to special types of personal information.
3. Personal information, de-identification and sensitive information	
Proposal 4.1 Change the word 'about' in the definition of personal information to 'relates to'. Ensure the definition is appropriately confined to where the connection between the information and the individual is not too tenuous or remote, through drafting of the provision, explanatory materials and OAIC guidance.	KPMG supports preserving the current definition of personal information and suggests instead that the existing guidance could be better utilised to provide more clarity about what personal information is, address industry-specific concerns and specific privacy risks. If this change is implemented, it will broaden the definition of personal information, which will require further consideration into the impacts of this change. For example, there will need to be consideration for the new types of personal information and how this may affect current deidentification, anonymisation, or pseudonymisation processes and requirements, as well as obligations in relation to data security and under the Notifiable Data Scheme.
Proposal 4.2 Include a non-exhaustive list of information which may be personal information to assist APP entities to identify the types of information which could fall within the definition. Supplement this list with more specific examples in the explanatory materials and OAIC guidance.	KPMG supports this proposal which seeks to provide more guidance and advice to APP entities interpreting the definition. Consideration should be given to ensure clarity that the list is non-exhaustive and that explanatory materials help entities interpret the concepts and rules.
Proposal 4.3 Amend the definition of 'collection' to expressly cover information obtained from any source and by any means, including inferred or generated information.	The current definition of personal information is sufficiently clear that inferred personal information is a form of personal information. However, we suggest that the Act could be amended to clarify whether specific obligations apply to inferred

	personal information, in particular whether the act of inferring personal information amounts to a collection of personal information ('collection by generation'). In our view, the Act is insufficiently clear on this point. While there are occasional references to inferred personal information in the OAIC's guidance,[3] the present review offers an opportunity for a clear policy and regulatory position to be taken on this issue.
Proposal 4.4 'Reasonably identifiable' should be supported by a non-exhaustive list of circumstances to which APP entities will be expected to have regard in their assessment.	As per the response to Proposal 4.2, KPMG supports providing increased guidance and advice to APP entities through the development of a non-exhaustive list of examples or circumstances. Care should be taken to avoid narrowing, even unintentionally, the objects of the Act in an attempt to address perceived limitations. Clearly defined concepts and rules, that are interoperable and are supported by the regulatory tools of code-making, guidance and advice, together with a strong regulator, should be preferred as the most effective means for enabling compliance and be assessed as part of a comprehensive Regulatory Impact Statement process.
Proposal 4.5 Amend the definition of 'de-identified' to make it clear that de-identification is a process, informed by best available practice, applied to personal information which involves treating it in such a way such that no individual is identified or reasonably identifiable in the current context.	KPMG supports the clarification proposed in this definition that seeks to provide clarity on what constitutes de-identified data. KPMG notes that further clarity about the concept of 'de-identified' information may be better governed under industry-specific codes and should be the subject of further guidance which also allows flexibility to evolve. Further, it would be beneficial to provide for evolving regulatory guidance about what methods are accepted within the Australian context. Providing clear guidance will allow APP entities to implement the appropriate mechanisms to ensure data is de-identified or rendered anonymous to provide certainty about what guidance or frameworks may be applied. In KPMG's view the question of whether de-identified information should be regulated in the same way as personal information requires closer consideration.
Proposal 4.6 Extend the following protections of the Privacy Act to de-identified information: APP 11.1 – require APP entities to take such steps as are reasonable in the circumstances to protect de-identified information: a) from misuse, interference and loss; and b) from unauthorised re-identification, access, modification or disclosure. APP 8 – require APP entities when disclosing de-	The proposed requirement to protect 'de-identified information', including aggregated information, within Australia and when disclosed cross-borders, is a substantial change likely to significantly impact organisations who routinely handle large amounts of de-identified information, including, but not limited to, those in health and research sectors, business intelligence and analytics (BI&A) or artificial intelligence (AI) industries, and digital communications and marketing.

[3] For example, Chapter B of the APP Guidelines states (para B.28) that 'Collection may also take place when an APP entity generates personal information from other data it holds, such as the generation of an audit log.'

identified information overseas to take steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles in relation to de-identified information, including ensuring that the receiving entity does not re- identify the information or further disclose the information in such a way as to undermine the effectiveness of the de-identification. Targeting proposals – the proposed regulation of content tailored to individuals should apply to de-identified information to the extent that it is used in that act or practice.	Further, the proposal to require entities to ensure that the overseas recipient does not breach the Australian Privacy Principles in relation to de-identified information needs to be considered in the context of what applicable obligations entities will have under the APPs in relation to de-identified information. This suggests that it is intended that de-identified information must be handled in the same way as personal information under the APPs.
Proposal 4.7 Consult on introducing a criminal offence for malicious re-identification of de-identified information where there is an intention to harm another or obtain an illegitimate benefit, with appropriate exceptions.	KPMG considers that reintroduction of the Privacy Amendment Re-identification Offence Bill 2016 should be considered with appropriate amendments. KPMG suggests a cautious approach given the potential for unintended consequences. The Bill also makes re-identification a criminal offence and carries potential serious consequences for those dealing with the types of personal information in scope, such as researchers. KPMG considers that any offence introduced should be very limited in scope with a high threshold that is targeted at malicious activity. Furthermore, we recommend greater clarity around the objective of this process and careful consideration of the flow on effects of such a significant change. This also needs to take into account the proposed introduction of the concept of 'anonymous'.
Proposal 4.8 Prohibit an APP entity from re-identifying de-identified information obtained from a source other than the individual to whom the information relates, with appropriate exceptions. In addition, the prohibition should not apply where: the re-identified information was de-identified by the APP entity itself - in this case, the APP entity should simply comply with the APPs in the ordinary way. the re-identification is conducted by a processor with the authority of an APP entity controller of the information.	KPMG supports OAIC's recommendation in its submission to the Discussion Paper[4] on introducing a prohibition on APP entities taking steps to re-identify information that they collected in an anonymised state, except to conduct testing of the effectiveness of security safeguards that have been put in place to protect the information. A further exception to the prohibition that KPMG suggests should be considered is where the individual has expressly consented to the process.
Proposal 4.9 Sensitive Information Amend the definition of sensitive information to include 'genomic' information. Amend the definition of sensitive information to replace the word 'about' with 'relates to' for consistency of terminology within the Act. Clarify that sensitive information can be inferred from information which is not sensitive information.	KPMG agrees with the proposal to include genomic information under the definition of sensitive information, however notes that due to the nature of genomic information and genomic sequencing, this information could arguably be used to identify individuals besides the person from which the genomic information was originally collected. KPMG notes that Australian Genomics and the Murdoch Children's Research Institute highlighted in past submissions that their organisations treat genomic information of

[4] https://www.oaic.gov.au/__data/assets/pdf_file/0023/11894/OAIC-submission-to-Privacy-Act~scussion-Paper-December-2021.PDF

	deceased individuals as being covered under the Act for this reason. Should the word 'about' be changed to 'relates to', it could assist organisations to identify that genomic information could relate to multiple individuals. However, this may also create additional complexity and confusion as to whether the information requires consent from all those to whom it relates. Given the complexity of such information, KPMG recommends that specific rules, provisions, and exemptions be considered and made clear in the Act, and that guidance be provided in relation to the use of genomic information. For example, specific rules around the use of genomic information should be drafted that consider how the information may relate to several individuals, and exemptions for the need to consent from all those individuals be included. As noted in response to Proposal 4.1, KPMG recommends that further consultation take place to understand the impacts that changing 'about' to 'relates to' may have as this would broaden the definition of personal information. This becomes uniquely challenging in relation to genomic information as the genomic sequence can 'relate to' multiple individuals. This creates complexity for organisations and brings into question whether consent is required from every individual to which the genomic sequencing 'relates'. As such, KPMG recommends the OAIC further consider the implications of changing the wording and consult with organisations who rely on sensitive and genomic information to ensure a change in wording does not have unintentional negative consequences. KPMG supports the proposal to clarify that sensitive information can be inferred from information which, by itself, is not sensitive. Given this scenario has occurred in relation to past data breaches, where the context of information allows for inferences to be made about an individual's sensitive information, KPMG recommends that guidance be provided to assist organisations in understanding when this can occur. The guidance should include case studies using past examples and exercises organisations can conduct to ascertain whether inferences can be made from their own data.
Proposal 4.10 Recognise collection, use, disclosure and storage of precise geolocation tracking data as a practice which requires consent. Define 'geolocation tracking data' as personal information which shows an individual's precise geolocation which is collected and stored by reference to a particular individual at a particular place and time, and tracked over time.	KPMG agrees that precise geolocation tracking should operate with consent, however, it should be made clear how precise such tracking data would need to be in order to meet the definition. For example, if a location that is tracked to a general area (e.g., a 10-kilometre radius) is classified in the same way as tracking to a precise location. Several modern mobile applications already implement such tracking which often asks for the end-user's consent. However, given the amount of information that can be derived from tracking an

	individual's location, more transparency is needed around how tracking data is used. An individual may not fully understand what they are consenting to – for instance, consent to track location to benefit from the application's functionality versus consent for tracking data to be used for additional purposes, such as marketing or sharing with other organisations. Additional consents should be considered for the use of tracking data for secondary purposes, particularly in relation to targeting the individual with personalised marketing. Entities should also adopt transparent practices that enable the individual to better understand how they are being tracked, how tracking data is used, and whether they can consent to being tracked only for certain purposes, without further use of the information. We note that geolocation may also be used to determine trusted identity and access, and therefore the purposes for which it is collected and when should be a consideration as well as the ability to provide services without it.
4. **Flexibility of the APPs**	
Proposal 5.1 Amend the Act to give power to the Information Commissioner to make an APP code where the Attorney General has directed or approved that a code should be made: where it is in the public interest for a code to be developed, and where there is unlikely to be an appropriate industry representative to develop the code. In developing an APP code, the Information Commissioner would: be required to make the APP Code available for public consultation for at least 40 days, and be able to consult any person he or she considers appropriate and to consider the matters specified in any relevant guidelines at any stage of the code development process.	KPMG supports this proposal in principle. It is KPMG's view that APP code-making powers are a preferred method of addressing discrete issues in the Act. However, KPMG recommends that the development of this power is approached cautiously to ensure the exercise of the power proposed is appropriately balanced against principles of natural justice. KPMG would support further consideration of the scope and threshold for the power to be exercised, with regard to the types of matters the OAIC would be empowered to make a code for, and to ensure the power is utilised as a last resort in circumstances where primary legislation amendments are unsuitable. For instance, it may be prudent to include non-exhaustive factors to be considered before determining whether it is in the public interest to develop a code, and a process for industry to have input. While KPMG agrees with a mechanism to allow for public consultation to ensure transparency, we would support a review mechanism through an external body to ensure that the scope of the code remains in alignment with the purposes and principles of the Act - particularly in circumstances where a code would affect the privacy rights of individuals.
Proposal 5.2 Amend the Act to enable the Information Commissioner to issue a temporary APP code for a maximum 12 month period on the direction or approval of the Attorney-General if it is	For similar reasons as discussed above, KPMG supports the proposal in principle, but would also support further clarification on the circumstances where a temporary APP code would be 'urgently' required and in the public interest.

urgently required and where it is in the public interest to do so.	KPMG notes that 12 months, despite being a maximum period, is a significant amount of time. KPMG recommends exploring safeguards to reduce the risk of this power being used inappropriately, balanced against any urgent need to enact it. This is critical given the lack of public consultation proposed in contrast to Proposal 5.1. By way of example, KPMG would support a review period immediately after a temporary code is implemented, that could allow it to be revoked in circumstances where the result of the review found that it was to fall outside the scope and objectives of the Act, and/or could negatively impact the privacy rights of individuals.
Proposal 5.3 Amend the Act to enable Emergency Declarations to be more targeted by prescribing their application in relation to: entities, or classes of entity classes of personal information, and acts and practices, or types of acts and practices.	KPMG supports the proposal in circumstances where the Emergency Declarations are more targeted. We would welcome further guidance on the circumstances in which such declaration can be made (i.e., the scope of the emergencies), or further exploration of non-binding factors to consider before a declaration is made. KPMG would also support a requirement for 80L of the Act to be amended and clearly specify that Emergency Declarations made against a specific entity or class of entity are also publicly accessible. This would ensure that any targeted application to a specific entity or class of entity is sufficiently transparent and in line with the principles of the proposal.
Proposal 5.4 Ensure the Emergency Declarations are able to be made in relation to ongoing emergencies.	KPMG supports the proposal in principle, and assumes that there will be a minimum standard in determining the types of laws that are comparable. KPMG would welcome further guidance on circumstances where some but not all privacy protections affected by an Emergency Declaration has a comparable state or territory law in place and otherwise refers to our submissions above.
Proposal 5.5 Amend the Act to permit organisations to disclose personal information to state and territory authorities under an Emergency Declaration, provided the state or territory has enacted comparable privacy laws to the Commonwealth.	KPMG understands that there are currently mechanisms in place to allow the disclosure of personal information if health or safety are at risk. We support the release of personal information under an Emergency Declaration, while noting the following considerations: • Further clarity on what is considered comparable privacy laws to the Commonwealth; • Appropriate guardrails are put in place to ensure personal information is handled appropriately, including protections around retention of data; and • A clear and agreed process for the disclosure of this information under an Emergency Declaration.

5. Small business exemption	
Proposal 6.1 Remove the small business exemption, but only after: a) an impact analysis has been undertaken to better understand the impact removal of the small business exemption will have on small business - this would inform what support small business would need to adjust their privacy practices to facilitate compliance with the Act b) appropriate support is developed in consultation with small business c) in consultation with small business, the most appropriate way for small business to meet their obligations proportionate to the risk, is determined (for example, through a code), and d) small businesses are in a position to comply with these obligations.	KPMG considers that removing the small business exemption must be undertaken in a well-planned and consultative manner, and subject to a comprehensive Regulatory Impact Statement. Changes to this exemption will have a significant impact particularly given the expansion of the privacy regulatory framework across the data lifecycle in the private sector and imposing additional regulation that may not always be proportionate to the privacy risk at every stage for all types of small businesses. Given this, it may be beneficial to consider removing the exemption in a phased approach that begins with higher-risk businesses. The purpose of its removal, whether this happens in whole or in part, and the economic impact this would have requires careful consideration and an assessment of how any changes will interact with other aspects of the current regulatory framework and reform that is implemented, including changes to cyber security regulations as a result of the Cyber Security Strategy. KPMG recommends that a mechanism to bring together the implementation of various regulations will be critical, to ensure it is done in a way that considers the impost on areas of the economy that are already under strain. It will be important to ensure that adequate support is provided to businesses to help them prepare for changes to this exemption, including education programs. KPMG suggests that bringing people together through appropriate professional bodies or forums such as the Council of Small Business Organisations Australia (COSBOA) or the Australian Small Business and Family Enterprise Ombudsman (ASBFEO) would be an efficient way to support businesses through the changes.
Proposal 6.2 In the short term: a) prescribe the collection of biometric information for use in facial recognition technology as an exception to the small business exemption, and b) remove the exemption from the Act for small businesses that obtain consent to trade in personal information.	KPMG supports these measures in principle, given these activities carry a high privacy risk. However, before these measures are implemented, further clarity and guidance should be provided on how this proposal will operate in practice. One mechanism that could be considered when implementing these measures is leveraging cloud-based platforms who could provide these protections as part of their services to small businesses. These companies are often well placed to comply with privacy obligations, stay up to date with advances in technology and regulation, and could use this service as a differentiator in the market.

6. Employee records exemption	
Proposal 7.1 Enhanced privacy protections should be extended to private sector employees, with the aim of: a) providing enhanced transparency to employees regarding what their personal and sensitive information is being collected and used for b) ensuring that employers have adequate flexibility to collect, use and disclose employees' information that is reasonably necessary to administer the employment relationship, including addressing the appropriate scope of any individual rights and the issue of whether consent should be required to collect employees' sensitive information c) ensuring that employees' personal information is protected from misuse, loss or unauthorised access and is destroyed when it is no longer required, and d) notifying employees and the Information Commissioner of any data breach involving employee's personal information which is likely to result in serious harm. Further consultation should be undertaken with employer and employee representatives on how the protections should be implemented in legislation, including how privacy and workplace relations laws should interact. The possibility of privacy codes of practice developed through a tripartite process to clarify obligations regarding collection, use and disclosure of personal and sensitive information should also be explored.	KPMG notes that it is unclear at this stage how these protections will work in practice, for example under the consent and notice obligations in the current framework of APPs 3, 5 and 6. The review acknowledges the challenges of the application of the GDPR lawful processing provisions in the context of the employer/employee relationship, which any reforms should have regard to. However, we support the protection of employee data and notification of any data breaches as outlined, noting that this is now a common best practice approach as recommended by the OAIC non-binding guidance. KPMG suggests that further consultation with small businesses is required when considering removing the employee records exemption in so far as it may apply to them, and the potential conflict with employment law and obligations to other employees in the workplace. In relation to b), the collection and handling of employee information would be for the primary purposes outlined and the review could consider the need for any additional permitted secondary purposes in the employment context given the complex range of obligations that employers have to ensure clarity. We refer to our comments above in relation to code-making, and while this supports flexible application of the privacy framework, it could lead to confusion around the standards and controls that would apply to employee information compared to other personal information. The recent data breaches have highlighted the connection between personal information of an individual in a private capacity and as an employee.
7. Political exemption	No KPMG comment.
8. Journalism exemption	No KPMG comment.
9. Privacy policies and collection notices	
Proposal 10.1 Introduce an express requirement in APP 5 that requires collection notices to be clear, up-to-date, concise and understandable. Appropriate accessibility measures should also be in place.	KPMG supports the introduction of an express requirement in APP 5 that collection notices be 'clear, up-to-date, concise and understandable', and to have 'appropriate accessibility measures' as outlined in Proposal 10.1. The proposed express requirement enhances the role of APP 5 as being distinct from APP 1, affirms the current APP Guidelines, aligns with the Australian Competition and Consumer Commission's (ACCC) Digital Platforms Inquiry Report, and better aligns with the GDPR. The replacement of 'current' with 'up-to-date', a requirement proposed in the Discussion Paper, should also not have a material impact on nor undermine the current flexibility of APP 5 on APP

	entities. Introducing the 'up-to-date' requirement should make it clear that APP entities must take steps to ensure they review and update collection notices when their practices have changed, and therefore efforts should remain 'effective in practice' and not 'impossible or disproportionate'. The distinction and interaction between a collection notice and a policy notice is made clear in the express requirement as it expands on collection notices being 'concise', a test that is not included in APP 1.4. KPMG considers that the 'concise' test would also "help[s] users make informed decisions" due to its succinct and easy-to-understand nature, and effectively support people who experience disabilities. Further, expanding the express requirement to include collection notices to be appropriately accessible, not just upon request, aligns with the GDPR's expectations of transparency and modalities and in effect builds on uniform data protection laws for online services.
Proposal 10.2 The list of matters in APP 5.2 should be retained. OAIC guidance should make clear that only relevant matters, which serve the purpose of informing the individual in the circumstances, need to be addressed in a notice. The following new matters should be included in an APP 5 collection notice: if the entity collects, uses or discloses personal information for a high privacy risk activity —the circumstances of that collection, use or disclosure that the APP privacy policy contains details on how to exercise any applicable Rights of the Individual, and the types of personal information that may be disclosed to overseas recipients.	KPMG welcomes the proposal to retain the list of matters in APP 5.2 (as previously recommended in our submission to the Discussion Paper) including maintaining the requirements in relation to any cross-border disclosure of personal information and disclosing whether the collection is required or authorised by law, while requiring only relevant matters to be included in notices that serve the purpose of informing the individual 'in the circumstances' with additional guidance from the OAIC. This would ensure flexibility for APP entities but also require them to determine and focus only on those matters that are relevant 'in the circumstances.' Further, having regard to the above, we also support the introduction of the proposed new matters to be listed in APP 5.2. This includes, the notification of high privacy risk activities, the detailing of applicable rights under APP 5 to the Privacy Policy, and the types of personal information that may be disclosed to overseas recipients. Specific to the notification of high privacy risk activities, we accept the inclusion of this new matter upon careful consideration and clear guidance from OAIC guidance under Proposal 13.3. We also support the corresponding Proposal 18, that would require an individual's rights to be disclosed at the point of collection in a meaningful way together with further information to be included in Privacy Policies about the procedures that support the exercise of these rights so that individuals can make an informed choice. Finally, we support the requirement to describe the types of personal information that may be disclosed to overseas recipients as part of the relevant matters. This will provide certainty for APP entities about what personal information can be disclosed (as well as disclosing the specified

	countries under Proposal 23.5), enhance accountability and transparency under APP 8, and enable individuals to decide whether they wish to share their personal information in circumstances where it may be transferred overseas.
Proposal 10.3 Standardised templates and layouts for privacy policies and collection notices, as well as standardised terminology and icons, should be developed by reference to relevant sectors while seeking to maintain a degree of consistency across the economy. This could be done through OAIC guidance and/or through any future APP codes that may apply to particular sectors or personal information-handling practices.	KPMG supports this proposal to develop standardised templates and layouts for privacy policies and collection notices, as well as standardised terminology and icons through OAIC guidance and/or any future APP codes. As noted in our response to the Discussion Paper, these initiatives would enhance user experience by helping them with informed decision-making due to language consistency across sectors, assist APP entities in drafting collection notices with pre-structured templates and terminology, and aligning industry standards across online platforms.
10. Consent and privacy default settings	
Proposal 11.1 Amend the definition of consent to provide that it must be voluntary, informed, current, specific, and unambiguous.	As stated in previous submissions, KPMG considers that the requirement for consent to be 'freely given' could be added to bring the Act into alignment with the GDPR. However, this would require an alternative lawful basis that APP entities could rely on where this would not be the case (for example in the employment relationship context), such as legitimate interest. In relation to the requirement that consent is 'current', guidance on how long a consent may be valid for and when renewal is required would be of assistance. The Spam Act addresses this to a limited extent in relation to direct marketing through electronic communications.
Proposal 11.2 The OAIC could develop guidance on how online services should design consent requests. This guidance could address whether particular layouts, wording or icons could be used when obtaining consent, and how the elements of valid consent should be interpreted in the online context. Consideration could be given to further progressing standardised consents as part of any future APP codes.	KPMG supports this proposal, including guidance on the specific circumstances for obtaining (layouts, wording or icons), recording and managing the consent to process the personal/sensitive information and what constitutes valid and current consent in the online context.
Proposal 11.3 Expressly recognise the ability to withdraw consent, and to do so in a manner as easily as the provision of consent. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.	KPMG considers that the ability for consent to be 'easily withdrawn' should be an element of the definition of valid consent, emphasising the need for entities to consider design mechanisms for consent withdrawal that are as easy as the provision of consent, and appropriately connected to the consent. KPMG considers that consumer choice and control, and the privacy tools that support the exercise of these, is an important aspect of establishing the right privacy settings in the context of a digital economy. The adoption and use of the concept of alternative applicable legal bases for processing personal information, such as legitimate interest, would also in our view help to

	enhance the interests of individuals in the management and control of their personal information and balance the increased burden that could be imposed on them by an over-reliance on consent as the lawful basis. This may also help to avoid difficulties where the need to continue to process certain personal information remains where consent may have been withdrawn. It will be important for individuals to understand the consequences of the withdrawal of their consent, such as the impact on their ability to receive certain online services, and guidance for APP entities about whether they are required to continue to provide any of the services on which the continued collection, use and/or disclosure of the personal information, that was the subject of the consent, was based.
Proposal 11.4 Online privacy settings should reflect the privacy by default framework of the Act. APP entities that provide online services should be required to ensure that any privacy settings are clear and easily accessible for service users.	KPMG supports this proposal, noting that it would bring APP entities in line with requirements in place for APP agencies under the Australian Government Agencies Privacy Code,[5] and with international regulations such as the GDPR. Further, we consider that online privacy settings should be included in the privacy by default framework in relation to geolocation data, service personalisation, data sharing and nudge techniques. All entities with online businesses should ensure privacy settings are clear and easily accessible for individuals to modify them, including making them the most restrictive and private. This will provide control, choice and help build trust. Additionally, KPMG considers that embedding the privacy by default framework as a principle across the APP framework would be an opportunity provide clarity to APP entities about the settings they are to operate within. This would also help guide the enforcement of the APPs by the OAIC.
11. Fair and reasonable personal information handling	
Proposal 12.1 Amend the Act to require that the collection, use and disclosure of personal information must be fair and reasonable in the circumstances. It should be made clear that the fair and reasonable test is an objective test to be assessed from the perspective of a reasonable person.	KPMG supports this proposal. In KPMG's view, an overarching 'fair and reasonable' test is an appropriate one that still allows flexibility and an assessment of the circumstances of use and disclosure, and allows a balanced approach. However further guidance on what fairness means in this context is recommended to ensure it aligns with other relevant frameworks that have adopted the fairness test, given the wide range of contexts in which personal information is collected and handled.
Proposal 12.2 In determining whether a collection, use or disclosure is fair and reasonable in the circumstances, the following matters may be taken into account: a) whether an individual would reasonably expect	KPMG supports the approach of providing guidance on this topic, noting that the list should not be exhaustive and should also take into account and clarify the circumstances where disclosure is required or authorised by law.

[5] https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/government-agencies/australian-government-agencies-privacy-code/about-the-australian-government-agencies-privacy-code

the personal information to be collected, used or disclosed in the circumstances b) the kind, sensitivity and amount of personal information being collected, used or disclosed c) whether the collection, use or disclosure is reasonably necessary for the functions and activities of the organisation or is reasonably necessary or directly related for the functions and activities of the agency d) the risk of unjustified adverse impact or harm e) whether the impact on privacy is proportionate to the benefit f) if the personal information relates to a child, whether the collection, use or disclosure of the personal information is in the best interests of the child, and g) the objects of the Act. The EM would note that relevant considerations for determining whether any impact on an individual's privacy is 'proportionate' and could include: a) whether the collection, use or disclosure intrudes upon the personal affairs of the affected individual to an unreasonable extent b) whether there are less intrusive means of achieving the same ends at comparable cost and with comparable benefits, and c) any actions or measures taken by the entity to mitigate the impacts of the loss of privacy on the individual.	
Proposal 12.3 The requirement that collection, use and disclosure of personal information must be fair and reasonable in the circumstances should apply irrespective of whether consent has been obtained. The requirement that collection, use and disclosure of personal information must be fair and reasonable in the circumstances should not apply to exceptions in APPs 3.4 and 6.2. The reference to a 'fair means' of collection in APP 3.5 should be repealed.	KPMG seeks further clarification on this proposal, as these proposals appear to be inconsistent as consent is a lawful basis or permitted exception to the collection and handling of personal information in APP 6.2. KPMG agrees that the overarching consideration of the circumstances should be a requirement across the collection, use and disclosure of that data.
12. Additional protections	
Proposal 13.1 APP entities must conduct a Privacy Impact Assessment for activities with high privacy risks. a) A Privacy Impact Assessment should be undertaken prior to the commencement of the high-risk activity. b) An entity should be required to produce a Privacy Impact Assessment to the OAIC on request.	Subject to the below, KPMG supports proposal 13.1(a), noting this would have the effect of bringing APP entities in line with requirements in place for APP agencies under the Privacy Code, and with international regulations such as the GDPR. KPMG supports the extension of that requirement to the private sector, where inherently 'high-risk activities' are explained in OAIC guidance, rather than enshrined in the Act, to support the enduring nature of reforms and future-proof in the face of the evolving digital age.

The Act should provide that a high privacy risk activity is one that is 'likely to have a significant impact on the privacy of individuals'. OAIC guidance should be developed which articulates factors that that may indicate a high privacy risk, and provides examples of activities that will generally require a Privacy Impact Assessment to be completed. Specific high risk practices could also be set out in the Act.	While the OAIC has regulatory powers to compel the production of documents, such as in the investigation of a complaint, proposal 13.1(b) expressly requires the record keeping of completed Privacy Impact Assessments (PIAs). Any enactment of the proposal should contemplate the longevity and future-reaching nature of this regulatory power, in the context of how long PIAs may be required to be kept and maintained, and also commercial in confidence obligations.
Proposal 13.2 Consider how enhanced risk assessment requirements for facial recognition technology and other uses of biometric information may be adopted as part of the implementation of Proposal 13.1 to require Privacy Impact Assessments for high privacy risk activities. This work should be done as part of a broader consideration by government of the regulation of biometric technologies.	As set out in responses to the Issues Paper and Discussion Paper, KPMG notes that biometric data is increasingly captured and used for a range of purposes in digital form by APP agencies and APP entities, including facial recognition, and there are associated privacy risks. Several moratoria are currently in place in various jurisdictions in relation to the development and use of 'biometric technologies', in particular facial recognition technology (FRT) (comprising software, AI and other surveillance mechanisms). As such, this is a specific area that requires further consideration, given the privacy risks and impacts and the current absence of any express provisions for the permitted collection and used of biometric data and the rights of individuals that may be impacted. We refer to KPMG's March 2020 submission *Human Rights and Technology in 2020 and Beyond* for a more detailed assessment of the privacy implications of emerging technology.[6] Restating our position outlined in the Discussion paper, KPMG considers that APP code-making powers and related guidance in the Act may provide a more appropriate mechanism to target and address certain industries or practices, rather than enshrining, at a point in time, particular technologies or practices that may be considered high risk and addressing these elements in legislation. This may also include the basis on which law enforcement and security agencies may be permitted to collect and use this data and obligations to keep it secure. Biometric data can also be used as a form of verifying an individual's identity to enable them to access services, systems, accounts or information. While this supports the establishment of trusted digital identity, there is currently no established legislative framework (such as in relation to the Trusted Digital Identity Framework) that expressly addresses the risks from the use of biometric data in this way, given that it is so unique to the individual and cannot be replaced if compromised.
Proposal 13.3 The OAIC should continue to develop practice-specific guidance for new technologies and emerging privacy risks. Practice-specific guidance could outline the OAIC's	KPMG supports the development of practice-specific guidance relating to new and emerging technologies, and their associated novel privacy risks. Clarity provided through regulatory guidance

[6] https://humanrights.gov.au/sites/default/files/2020-07/34_-_kpmg_australia_1.pdf

expectations for compliance with the Act when engaging in specific high-risk practices, including compliance with the fair and reasonable personal information handling test.	would assist in establishing a clear baseline and benchmark, supporting implementation and assessment in this context, and managing expectations relating to OAIC's prospective regulatory action. This may also be supported by other bodies or institutions with the relevant expertise in relation to emerging technologies including the application of ethical frameworks.
Proposal 13.4 Include an additional requirement in APP 3.6 to the effect that where an entity does not collect information directly from an individual, it must take reasonable steps to satisfy itself that the information was originally collected from the individual in accordance with APP 3. OAIC guidelines could provide examples of reasonable steps that could be taken.	In response to the Discussion Paper, KPMG noted that this proposal does not appear to take into account insights derived from or inferred from personal information that has already been collected. As such, in its current form, introduction of the requirement may lead to ambiguity and a burden on implementing organisations. KPMG restates its overarching position that systems relating to information collected indirectly need to remain practicable. KPMG notes that the current system appropriately places the onus on the APP entity collecting the information (or on whose behalf the information is being collected and is likely to have the most direct relationship with the individual) to properly assess its own compliance with APP 3.
13. Research	
Proposal 14.1 Broad consent for research Introduce a legislative provision that permits broad consent for the purposes of research: a) Broad consent should be available for all research to which the research exceptions in the Act (and proposed by this chapter) will also apply. b) Broad consent would be given for 'research areas' where it is not practicable to fully identify the purposes of collection, use or disclosure of personal or sensitive information at the point when consent is being obtained.	KPMG agrees with the limitations of the current requirements for consent to be 'current' and 'specific' due to factors such as the evolving and potentially indeterminate future uses of personal or sensitive information in research, the impact of technology and the size and distribution of the participant cohort. The need to obtain this type of consent can add a significant burden to certain types of research programs that are in the public interest as the needs of the population and research discoveries evolve. KPMG supports the proposal in 14.1 (a) to introduce the concept of 'broad consent' in a manner similar to the GDPR. However, its permitted use should be constrained by parameters such as being limited to use in circumstances where: a) the research exceptions in the Act apply; and b) the utility in conducting indeterminate/unspecified future research has been justified and accepted by a qualified Human Research Ethics Committee (HREC) subject to any appropriate conditions. More guidance should be issued on future indeterminate/unspecified public interest research to ensure that the concept of broad consent cannot be applied too flexibly or misused, and/or is only a last resort option for when research purpose(s) cannot demonstrably be reasonably ascertained at the time the personal information is collected. We agree with guidance provided in Recital 33 to the GDPR by the European Commission Data Protection Working Party which states that broad

	consent should not replace specific consent and individuals should still be provided with the opportunity to give specific consent to certain research areas where possible.[7] KPMG supports the application of the same/similar guidance in Australia. Further, it is appropriate that any reliance on broad consent should be supported by an analysis that must weigh the burden of seeking express, valid consent retrospectively from individuals – both on the individuals themselves and on the research project and objectives. This should be justified to HRECs on a case-by-case basis and guidance should be issued on the relevant considerations that must be addressed when undertaking such an assessment. These should be similar to those currently considered when assessing whether it is impracticable to seek an individual's consent in accordance with section 16B(2) and (3) of the Act. As previously raised in our submissions, the current fragmented state of health information regulation is also an important consideration as HRECs are often considering the application of both the Act and state-based obligations in the research context, which do not always align and can cause an undue burden and complexity for the research and individuals.
Proposal 14.2 Consult further on broadening the scope of research permitted without consent for both agencies and organisations.	KPMG considers that obtaining meaningful and lawful consent in relation to the processing of all types of personal information is not always possible or practical and can place more burden on individuals. However, broadening the scope of research permitted without consent could remove individual choice and control in relation to the ongoing use of their sensitive information (such as health information in the case of medical research). There is already a research exemption which can support progressing certain research projects without consent (i.e., as long as the criteria are satisfied) under sections 95 and 95A of the Privacy Act. KPMG would instead propose that the current guidelines and conditions in the Act that support the exemption are further developed and clarified to outline the circumstances in which the relevant information collected may be permitted to be used. We also refer to our submissions above in relation to Proposal 14.1.
Proposal 14.3 Consult further on developing a single exception for research without consent and a single set of guidelines, including considering the most appropriate body to develop the guidelines.	KPMG supports further consultation on combining the research exceptions and developing one set of research guidelines. We note that the two sets of guidelines establish inconsistent standards for different types of personal information depending on APP entity type (i.e., section 95 applies to personal information more broadly and allows agencies to circumvent the APPs for medical

[7] https://gdpr-info.eu/recitals/no-33/

	research. Section 95A, however, applies to organisations' collection, use and disclosure of personal information only for research/compilation of stats relevant to health or public safety). KPMG considers that the safeguards that apply to medical research will need to be embedded just as strongly in a unified guideline as they would in the current separate ones. As such, we support the submissions made by the Australian Law Reform Commission with respect to the Privacy Commissioner being well-placed to play a coordinating role in the development of new guidelines.
14. Organisational Accountability	
Proposal 15.1 An APP entity must determine and record the purposes for which it will collect, use and disclose personal information at or before the time of collection. If an APP entity wishes to use or disclose personal information for a secondary purpose, it must record that secondary purpose at or before the time of undertaking the secondary use or disclosure.	KPMG supports this proposal which introduces further organisational accountability requirements into the Act. This proposal aligns with GDPR requirements, and supports accountability and compliance with proposed expanded rights such as explanation. Recording the purposes for which an entity will collect, use and disclose personal information will also support data retention compliance.
Proposal 15.2 Expressly require that APP entities appoint or designate a senior employee responsible for privacy within the entity. This may be an existing member of staff of the APP entity who also undertakes other duties.	KPMG supports in principle the accountability by senior employees in an organisation who are responsible for privacy, given that sufficient standing within an organisation is required to influence or develop a privacy program and provide advice. KPMG recommends that this does not have to be a single individual, and could also be a designated team who shares this responsibility.
15. Children	
Proposal 16.1 Define a child as an individual who has not reached 18 years of age.	KPMG supports the proposed definition of a child as a person below the age of 18 years unless majority is attained earlier under applicable law. This would make it consistent with other relevant legislation including the Online Privacy code.
Proposal 16.2 Existing OAIC guidance on children and young people and capacity should continue to be relied upon by APP entities. An entity must decide if an individual under the age of 18 has the capacity to consent on a case-by- case basis. If that is not practical, an entity may assume an individual over the age of 15 has capacity, unless there is something to suggest otherwise. The Act should codify the principle that valid consent must be given with capacity. Such a provision could state that 'the consent of an individual is only valid if it is reasonable to expect that an individual to whom the APP entity's activities are directed would understand the nature, purpose and consequences of the collection, use	KPMG restates our response to the Discussion Paper that a specific age may be too prescriptive and restrictive, without considering the subjective capacity of a minor in the circumstance and the context in which they are exercising their rights. KPMG supports the need for an APP entity to have the ability to make a case-by-case assessment about whether an individual under the age of 18 has the capacity to consent (having regard to the proposed updated definition of lawful consent in Proposal 11.1) and for entities to be able to rely on the assumption that an individual over the age of 15 has capacity unless there are circumstances to suggest otherwise. KPMG considers that further clarity should be provided on how the age of 15 has been determined as the appropriate assumed

or disclosure of the personal information to which they are consenting.' Exceptions should be provided for circumstances where parent or guardian involvement could be harmful to the child or otherwise contrary their interests (including, but not limited to confidential healthcare advice, domestic violence, mental health, drug and alcohol, homelessness or other child support and community services).	age of capacity for exercising privacy rights or providing consent. KPMG welcomes additional guidance from the OAIC upon the circumstances that would mean an individual over the age of 15 lacks the capacity to consent. KPMG also supports the proposal to include exceptions for circumstances where parent or guardian involvement could be harmful to the child or otherwise contrary to their interests. These exceptions should be expressly written into the Act and be aided by general guidance from the OAIC on how these exceptions may apply practically. For example, in the context of familial legal disputes.
Proposal 16.3 Amend the Privacy Act to require that collection notices and privacy policies be clear and understandable, in particular for any information addressed specifically to a child. In the context of online services, these requirements should be further specified in a Children's Online Privacy Code, which should provide guidance on the format, timing and readability of collection notices and privacy policies.	KPMG supports the standardisation of collection notices and privacy policies so they are clear and understandable, in particular for any information addressed specifically to a child which would enhance user experience and help users make informed decisions having regard to their age and circumstances.
Proposal 16.4 Require entities to have regard to the best interests of the child as part of considering whether a collection, use or disclosure is fair and reasonable in the circumstances.	KPMG has supported an overarching fair and reasonable test as the appropriate baseline test for considering the privacy interests of individuals as it still allows a balanced and flexible approach and an assessment of the circumstances of the proposed use or disclosure and having regard to our response to the proposed amendments to the objects of the Privacy Act.
Proposal 16.5 Introduce a Children's Online Privacy Code that applies to online services that are 'likely to be accessed by children'. To the extent possible, the scope of an Australian children's online privacy code could align with the scope of the UK Age Appropriate Design Code, including its exemptions for certain entities including preventative or counselling services. The code developer should be required to consult broadly with children, parents, child development experts, child- welfare advocates and industry in developing the Code. The eSafety Commissioner should also be consulted. The substantive requirements of the Code could address how the best interests of child users should be supported in the design of an online service.	KPMG refers to comments in Section 20 of this response.
16. People experiencing vulnerability	
Proposal 17.1 Introduce, in OAIC guidance, a non-exhaustive list of factors that indicate when an individual may be experiencing vulnerability and at higher risk of harm from interferences with their personal information.	KPMG supports the proactive approach to improved privacy protections for all people experiencing vulnerability at any stage and welcomes non-exhaustive guidance on factors that indicate when an individual may be experiencing

	vulnerability, as it may not necessarily be a persistent state. KPMG considers that further guidance from the OAIC may assist APP entities to take appropriate steps to manage risks associated with people experiencing vulnerability including in the context of the activities undertaken by entities in particular sectors, such as the finance sector. The introduction of guidance should not be overly prescriptive as this may result in an increased and disproportionate regulatory burden for APP entities. Instead, it should be broad enough to assist the entities to adequately support vulnerable individuals to make informed choices about their personal information. This could also be supplemented by sector specific guidance. Also note our response to Proposal 17.3 below.
Proposal 17.2 OAIC guidance on capacity and consent should be updated to reflect developments in supported decision- making.	KPMG supports the need for updated guidance for supported decision-making and to provide greater clarity on when and how third parties who give decision-making support should be recognised, and what steps APP entities should take to ensure that authorities, nominations and consents are valid, including the provision of supporting collection notices. Such guidance should not create disproportionate regulatory burden.
Proposal 17.3 Further consultation should be undertaken to clarify the issues and identify options to ensure that financial institutions can act appropriately in the interests of customers who may be experiencing financial abuse or may no longer have capacity to consent.	The circumstances in which individuals may experience vulnerability are complex and their manifestation in the privacy context may differ across sectors, such as in the context of financial abuse. KPMG supports the need to prevent financial abuse and further consultation and consideration into helping financial institutions act appropriately and in the best interest of customers to identify privacy issues and potential solutions that achieve the right balance.
17. Rights of the Individual	
Access and Explanation **Proposal 18.1** Provide individuals with a right to access, and an explanation about, their personal information if they request it, with the following features: a) an APP entity must provide access to the personal information they hold about the individual (this reflects the existing right under the Act) b) an APP entity must identify the source of the personal information it has collected indirectly, on request by the individual c) an APP entity must provide an explanation or summary of what it has done with the personal information, on request by the individual d) the entity may consult with the individual about the format for responding to a request, and the	(a) Right of access is correctly observed as a first hurdle and necessary to support many other rights of individuals. Without access to personal information, individuals would be unable to determine whether they are impacted and how. This amendment also brings the Act into line with the GDPR and other harmonisation efforts globally. (b) KPMG supports this proposal in principle from a transparency perspective, and considers that access rights should include understanding what information was collected indirectly. KPMG notes that it may not always be practicable for an entity to identify the source of the personal information it has collected. (c) The provision of explanation under 18.1(c) should be supplemented with further guidance from the OAIC in relation to the context in which an organisation should be providing more detailed

format should reflect the underlying purpose of ensuring the individual is informed, as far as is reasonable, about what is being done with their information e) an organisation may charge a 'nominal fee' for providing access and explanation where the organisation has produced a product in response to an individual	summaries as opposed to a high-level summary also having regard to, for example, the exceptions in APP 12.2. This will help reduce costs and resource burden and support greater efficiency for furtherance of access rights. (d) This section is drafted as an option not as a directive and therefore provides good practice. As it is not mandatory, it is appropriate based on each case that a company faces. (e) The term nominal is important so that the right of access is not compromised and there are no cost barriers or burdens on individuals (in particular for individuals experiencing financial hardship). However, this also needs to the proportionate to the costs entities may incur responding to persistent or voluminous requests, having regard to the nature of digital data and how it may be stored. To address this, KPMG suggests refinements to APP 12, to reflect some of qualifications in the Freedom of Information Act, such as the ability to decline access requests from individuals if meeting those requests will unduly divert resources. Instead, we propose requiring entities and individuals to work together to refine the scope of their access/correction requests. The narrowing of the employee record and removal of small business exemption and the application of these rights and corresponding obligations on employers and small businesses needs to be considered in the context of the impact of the exercise of individual access requests under the GDPR, which suggests the most pronounced impact in practice is in the context of access request responses to ex/employee data subjects.
Objection **Proposal 18.2** Introduce a right to object to the collection, use or disclosure of personal information. An APP entity must provide a written response to an objection with reasons.	The right to object to collection or use is a necessary extension of the access right as it allows individuals to elect to request changes to the practices of the entities holding their information (e.g., opt out of marketing, limit personal information collection of a sensitive nature). It also provides feedback to entities on consumer expectations to inform their ongoing data collection and governance practices. This amendment also brings the Australian Privacy Act into line with the GDPR and other harmonisation steps globally. However, more guidance is needed on how to ensure the effective exercise of these rights, and how to limit demands that may impose an unreasonable burden on the ability of the entity to carry out its functions and activities and to meet other public interests if the right is to be exercised, and to ensure the individuals understand the consequences of exercising those rights.
Erasure **Proposal 18.3** Introduce a right to erasure with the following features:	While KPMG supports the right in principle, we consider that there may not be an apparent need to introduce an additional and specific right to erasure at this time. The current data rights and

a) An individual may seek to exercise the right to erasure for any of their personal information. b) An APP entity who has collected the information from a third party or disclosed the information to a third party must inform the individual about the third party and notify the third party of the erasure request unless it is impossible or involves disproportionate effort. In addition to the general exceptions, certain limited information should be quarantined rather than erased on request, to ensure that the information remains available for the purposes of law enforcement.	the regulatory powers of the OAIC that require personal information to be deleted in appropriate circumstances should be sufficient. We also note the high degree of complexity that the application of this right has had under the GDPR. However, KPMG acknowledges that any introduction of a specific right to erasure would support the principles of data minimisation and giving individuals further control over their data and clarity for entities about their obligations. If an express additional right is introduced, we would recommend this is done after further careful consideration of the outcomes and the experience under the GDPR to inform the formulation of the right and applicable exceptions and to ensure individuals understand that the right is not absolute.
Correction **Proposal 18.4** Amend the Act to extend the right to correction to generally available publications online over which an APP entity maintains control.	KPMG supports this right in principle, consistent with the right to correction that already exists. However, this may not always be practicable or reasonable and there may be appropriate exceptions that entities may rely on. KPMG therefore recommends further clarity is provided about how this right would be formulated.
De-indexing **Proposal 18.5** Introduce a right to de-index online search results containing personal information which is: a) sensitive information [e.g. medical history], or b) information about a child, or c) excessively detailed [e.g. home address and personal phone number], or d) inaccurate, out-of-date, incomplete, irrelevant, or misleading. The search engine may refer a suitable request to the OAIC for a fee. The right should be jurisdictionally limited to Australia.	Whilst this relates only to online search results and therefore primarily impacts digital platform providers, there is a risk that accurate and true information is deleted which is otherwise in the public interest to remain available as a matter of record or to ensure that overall, the records in the results are complete. This proposal should also be considered against other matters of public interest and the practical reality that search is the means by which everyone is effectively able to access information on the internet, enables its free flow, and support rights such as freedom of information. The search platform who would be required to undertake the de-indexing may also not have all the available information to consider whether a de-indexing request is appropriate in each circumstance. The primary question should be whether the information should be permitted to be available online to be disclosed to the world at large, considering the nature of the entity publishing the information that is captured in the search results, the applicable APP and/or other relevant obligations (including the proposed additional fair and reasonable test and the obligations relating to children). However, KPMG also acknowledges the impact that the publication of certain categories of information, that may readily be available globally, may have on individuals. KPMG recommends that further consideration should be given to the development of such a right and the potential adverse impacts on other rights and public interest matters, the availability of other rights in relation to

	correction and deletion, as well as the mechanisms by which individuals can raise their concerns about the publication of such information in search results.
Exceptions **Proposal 18.6** Introduce relevant exceptions to all rights of the individual based on the following categories: a) Competing public interests: such as where complying with a request would be contrary to public interests, including freedom of expression and law enforcement activities. b) Relationships with a legal character: such as where complying with the request would be inconsistent with another law or a contract with the individual. c) Technical exceptions: such as where it would be technically impossible, or unreasonable, and frivolous or vexatious to comply with the request.	KPMG maintains that any decision to proceed to insert a direct individual right of action should be carefully considered against the introduction of the expanded rights that have been proposed, as well as the introduction of a statutory tort of privacy. KPMG broadly supports the introduction of the general exceptions to the exercise of the proposed expansion of privacy rights outlined in Proposal 18 which aim to be consistent with the exceptions in the current permitted heath and general situations and we refer to our response to Proposal 18.5 above. In relation to 18.6 (a), we consider it appropriate that the application of this exception is subject to a balancing of competing public interests including those that the relevant activities of the APP entity support. The amendment to the objects of the Act will be a relevant consideration. We consider that there may be a broad range of potentially competing public interests relevant to the exercise of a range of proposed rights. Therefore, we support further guidance from the OAIC on the relevant factors to be considered when undertaking such an assessment that reflect the further consultation recommended, and would also support further clarity in the legislation on this matter. In regard to 18.6 (b) we agree that the rights of the individual should not interfere with or displace the law, or conflict with collection, use, disclosure, or the retention of information which is required or authorised by law. Therefore, we support the introduction of this exception to the rights of the individual. In relation to 18.6 (c) we consider it appropriate that there is an exception for technical limitations where it would be technically impossible, unreasonable, or frivolous or vexatious to comply with the request and refer to our submissions to Proposal 18.1 above. However, this should be supported clear guidelines from the OAIC on the extent to which the exception can be relied on.
Response **Proposal 18.7** Individuals should be notified at the point of collection about their rights and how to obtain further information on the rights, including how to exercise them. Privacy policies should set out the APP entity's procedures for responding to the rights of the individual.	18.7) KPMG supports the proposal that individuals are notified about their rights and how to obtain further information about them at the point of collection. However, we propose that the matters currently required to be addressed in both APP 5 notices and privacy policies be amended to include this information without creating overly onerous additional notification requirements at the point of collection. 18.8) KPMG supports the obligation of reasonable assistance and submit that providing an

Proposal 18.8 An APP entity must provide reasonable assistance to individuals to assist in the exercise of their rights under the Act. **Proposal 18.9** An APP entity must take reasonable steps to respond to an exercise of a right of an individual. Refusal of a request should be accompanied by an explanation for the refusal and information on how an individual may lodge a complaint regarding the refusal with the OAIC. **Proposal 18.10** An organisation must acknowledge receipt of a request to exercise a right of an individual within a reasonable time and provide a timeframe for responding. An agency and organisation must respond to a request to exercise a right within a reasonable timeframe. In the case of an agency, the default position should be that a reasonable timeframe is within 30 days, unless a longer period can be justified.	opportunity for an open dialogue between APP entities and consumers can assist consumers to better understand how their personal information is being used by the entity. This could also assist with compliance with APP 1 which requires transparency about the way personal information is managed. We consider that further guidance from the OAIC should be provided to assist APP entities to understand what would amount to reasonable assistance in the exercise of their rights. 18.9) KPMG broadly supports that an APP entity should be obliged to take reasonable steps to respond to requests to exercise the rights of an individual. However, we propose that guidance should be issued by the OAIC which assists entities to understand what considerations are accepted as 'reasonable'. 18.10) KPMG supports the obligation for an organisation to acknowledge their receipt of a request to exercise a right. However, we consider that if such rights are to be inserted into the Act, that APP entities may not immediately be adequately equipped to respond to the requests. That is, APP entities may need to consider cost and resourcing constraints associated with implementing capabilities to cover and respond to the additional rights. In turn, this may affect their ability to meet the 30-day timeframe. For this reason, we suggest that there should be flexibility for APP entities to justify to an individual why a response timeframe may be longer than 30 days.
18. Automated decision making	
Proposal 19.1 Privacy policies should set out the types of personal information that will be used in substantially automated decisions which have a legal or similarly significant effect on an individual's rights.	Policies in relation to automated decision making (ADM) should cover three key areas: • Transparency and consent to the use of personal information to carry out ADM and the types of ADM that the entity is making, having regard to Proposal 19.2; • The option to opt out from the use of personal information to carry out ADM; and • Ensure mitigation of data matching risk by taking into consideration the algorithms and processes that can reveal or leverage undisclosed, irrelevant, incorrect or incomplete personal information that would inform the outcome of the ADM.
Proposal 19.2 High-level indicators of the types of decisions with a legal or similarly significant effect on an individual's rights should be included in the Act. This should be supplemented by OAIC Guidance.	KPMG agrees that clarity about what types of ADM is considered to have this effect should be expressly defined in the Act and supplemented by further guidance from OAIC. Further, consideration should be given to introducing a requirement that any processing of personal information for ADM purposes must not have a material adverse impact on the rights of individuals – this would be consistent with GDPR and OECD privacy

	guidelines. An individual should, where possible, have the option to elect that their personal information is processed without recourse to ADM, that is, there is a human decision maker (both in whole and in part). Finally, KPMG notes that this is the subject of further investigation and as such, these obligations should not be introduced until that is completed.
Proposal 19.3 Introduce a right for individuals to request meaningful information about how substantially automated decisions with legal or similarly significant effect are made. Entities will be required to include information in privacy policies about the use of personal information to make substantially automated decisions with legal or similarly significant effect. This proposal should be implemented as part of the broader work to regulate AI and ADM, including the consultation being undertaken by the Department of Industry, Science and Resources.	KPMG's view is that this may require enhancement across different sectors. As an example, whilst the Credit Reporting Code specifically prohibits processing of credit information in certain circumstances (such as for example financial hardship), it does not place restraints on the use of ADM in the issuance of credit products. It may be pertinent to establish restraints and prohibitions on ADM in certain scenarios where there is a high risk of adverse impact. We agree that this proposal requires further consideration in the context of the work being undertaken by the Department of Industry, Science and Resources (DISR).
19. Direct marketing, targeting and trading	
Proposal 20.1 Amend the Act to introduce definitions for: a) **Direct marketing** – capture the collection, use or disclosure of personal information to communicate directly with an individual to promote advertising or marketing material. b) **Targeting** – capture the collection, use or disclosure of information which relates to an individual including personal information, deidentified information, and unidentified information (internet history/tracking etc.) for tailoring services, content, information, advertisements or offers provided to or withheld from an individual (either on their own, or as a member of some group or class). c) **Trading** – capture the disclosure of personal information for a benefit, service or advantage.	KPMG supports the introduction of new definitions and further consultation with businesses to refine and clarify these and when they would apply, and notes care must be taken in drafting these definitions so that they are broad enough to capture emerging technologies and ways of marketing and processing information, but in respect of: • "targeting" should not be so broad as to capture activities that are not intended to be targeting at a known individual; and • "trading" should not be so broad as to cover processing activities performed by a processor for a data controller or the sale of a business such as by shares/assets. We note the current definition of "targeting" as outlined in Proposal 20.1 is very broad and may catch broad based and segmented marketing. Amending the definition so that targeting requires using more than a set number of data elements about an individual will help address this concern.
Proposal 20.2 Provide individuals with an unqualified right to opt-out of their personal information being used or disclosed for direct marketing purposes. Similar to the existing requirements under the Act, entities would still be able to collect personal information for direct marketing without consent, provided it is not sensitive information and the individual has the ability to opt out.	KPMG supports the continuance of Australia's existing opt-out regulatory framework for marketing, on the basis that this strikes an appropriate balance between consumer empowerment and business continuity.

Proposal 20.3 Provide individuals with an unqualified right to opt-out of receiving targeted advertising.	KPMG supports this proposal subject to the comments made in response to Proposal 20.1. Additionally, given the nature of online business models that rely on the collection, use and sharing of data for targeting and personalisation to provide products and services at no cost, further consideration should be given to the consequences of this right and what individuals are told about what will happen when they exercise their right. It is also not clear whether the entity would be required to still provide the service or product once the right is exercised.
Proposal 20.4 Introduce a requirement that an individual's consent must be obtained to trade their personal information.	KPMG supports this proposal subject to the comments made in response to Proposal 20.1.
Proposal 20.5 Prohibit direct marketing to a child unless the personal information used for direct marketing was collected directly from the child and the direct marketing is in the child's best interests.	This is an important issue that requires careful consideration and consultation before its introduction, and as such government should consider not progressing this measure during the first stage of reforms.
Proposal 20.6 Prohibit targeting to a child, with an exception for targeting that is in the child's best interests.	
Proposal 20.7 Prohibit trading in the personal information of children.	
Proposal 20.8 Amend the Act to introduce the following requirements: a) Targeting individuals should be fair and reasonable in the circumstances. b) Targeting individuals based on sensitive information (which should not extend to targeting based on political opinions, membership of a political association or membership of a trade union), should be prohibited, with an exception for socially beneficial content.	KPMG's view is that targeting individuals based upon their sensitive information should be permitted with express consent and if the targeted content is reasonably believed to be individually beneficial to them. As an example, targeting individuals using health information may be individually beneficial but not sufficiently 'socially beneficial' as outlined in the proposal. Targeting in this way, where the targeting is intended to benefit them and is directly related to the primary purpose of the information collected, should be permitted if the individual has consented.
Proposal 20.9 Require entities to provide information about targeting, including clear information about the use of algorithms and profiling to recommend content to individuals. Consideration should be given to how this proposal could be streamlined alongside the consultation being undertaken by the Department of Industry, Science and Resources.	KPMG supports this proposal if coupled with the use of industry codes and further consultation with industry and the DISR.
20. Security, retention and destruction	
Proposal 21.1 Amend APP 11.1 to state that 'reasonable steps' include technical and organisational measures.	KPMG supports this proposal.

Proposal 21.2 Include a set of baseline privacy outcomes under APP 11 and consult further with industry and government to determine these outcomes, informed by the development of the Government's 2023-2030 Australian Cyber Security Strategy.	KPMG supports this proposal but notes the potential for consultation fatigue within industry and the urgency to get clarity on a way forward. We recommend that this proposal should be resolved through the development of the Government's Australian Cyber Security Strategy.
Proposal 21.3 Enhance the OAIC guidance in relation to APP 11 on what reasonable steps are to secure personal information. The guidance that relates to cyber security could draw on technical advice from the Australian Cyber Security Centre.	KPMG supports enhancing guidance in relation to APP 11, but recommends taking an evolutionary approach rather than waiting for a perfect solution given the urgency of providing guidance to industry, and the delayed updates to the OAIC Guidance on personal information security that was last published in 2018 and has been the subject of submissions.[8] We also note guidance that is already available, for example in relation to the Security of Critical Infrastructure Act, as well as the need to provide greater clarity for organisations of different sizes and risk sensitivities. KPMG would welcome a clear statement about the standards and frameworks that entities can reliably adopt and follow to achieve the required steps and outcomes.
Proposal 21.4 Amend APP 11.1 so that APP entities must also take reasonable steps to protect de-identified information.	See above response at Proposal 4.6.
Proposal 21.5 The OAIC guidance in relation to APP 11.2 should be enhanced to provide detailed guidance that more clearly articulates what reasonable steps may be undertaken to destroy or de-identify personal information.	See above response at Proposal 4.6.
Proposal 21.6 The Commonwealth should undertake a review of all legal provisions that require retention of personal information to determine if the provisions appropriately balance their intended policy objectives with the privacy and cyber security risks of entities holding significant volumes of personal information. This further work could also be considered by the proposed Commonwealth, state and territory working group at Proposal 29.3 as a key issue of concern where alignment would be beneficial. However, this review should not duplicate the recent independent review of the mandatory data retention regime under the Telecommunications (Interception and Access) Act 1979 and the independent reviews and holistic reform of electronic surveillance legislative powers.	KPMG welcomes this proposal for the Commonwealth to review all legal provisions that require the retention of personal information although acknowledges this is a significant undertaking. Entities large and small keep a range of personal information and records which may include it, to comply with a range of legislation. This includes various identity verification obligations such as the Anti-Money Laundering and Counter-Terrorism Financing Act (2006). A defined set of principles and guidelines to verify identity without needing to store that information will provide APP entities with greater clarity and certainty in approaching data storage, retention and destruction within its environment. This could be considered as part of the development of the Trusted Digital Identity Framework to ensure the two frameworks are harmonised.
Proposal 21.7 Amend APP 11 to require APP entities to establish their own maximum and minimum retention periods in relation to the personal information they hold which take into account the type, sensitivity and purpose of that	KPMG agrees with the report's reasoning for APP entities setting their own maximum and minimum retention periods. However, KPMG suggests APP 11 prescribes a requirement to implement appropriate technical and organisational measures

[8] https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/guide-to-securing-personal-information

information, as well as the entity's organisational needs and any obligations they may have under other legal frameworks. APP 11 should specify that retention periods should be periodically reviewed. Entities would still need to destroy or de-identify information that they no longer need.	for APP entities that hold significant volumes of personal information. This addition would further align APP 11 with international standards such as storage limitation principles under GDPR Article 5. A prescriptive requirement to APP 11 also strengthens the right to erasure as recommended by this report. KPMG welcomes the report's proposal to include periodic reviews and the requirement to destroy or de-identify information that they no longer need into APP 11.
Proposal 21.8 Amend APP 1.4 to stipulate than an APP entity's privacy policy must specify its personal information retention periods.	As per earlier submissions, KPMG supports the disclosure of retention periods in privacy notices and policy. To bring the Act into alignment with the GDPR, the storage period (or criteria to determine it) may be dictated by factors such as statutory requirements or industry guidelines but should be phrased in a way that allows the individuals to assess, on the basis of their own situation, what the retention period will be for specific data/ purposes. Further, any amendments to privacy notice and policy requirements must ensure that the regulatory burden is not disproportionate, with a focus on effective and meaningful disclosure through notices and transparency practices.
21. Controllers and processors of personal information	
Proposal 22.1 Introduce the concepts of APP entity controllers and APP entity processors into the Act. Pending removal of the small business exemption, a non-APP entity that processes information on behalf of an APP entity controller would be brought into the scope of the Act in relation to its handling of personal information for the APP entity controller. This would be subject to further consultation with small business and an impact analysis to understand the impact on small business processors.	KPMG considers that the concepts of APP entity controllers and APP entity processors into the Act are helpful, but the proposal is not clear on whether these will be introduced broadly, just for small businesses, or will vary. KPMG notes the impacts the introduction of these concepts may have on current contractual arrangements and any changes will need an appropriate lead in time.
22. Overseas data flows	
Proposal 23.1 Consult on an additional requirement in subsection 5B(3) to demonstrate an 'Australian link' that is focused on personal information being connected with Australia.	KPMG supports further clarification about the extraterritorial operation of the Privacy Act in light of the amendments made by the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 (Privacy Enforcement Bill). Given the application of the 'Australian link' test is applied to organisations operating across all industries and sectors, further consultation will be beneficial to ensure that there are no unintended consequences, especially where the establishment of an organisation's connection with Australia may be complex.

Proposal 23.2 Introduce a mechanism to prescribe countries and certification schemes as providing substantially similar protection to the APPs under APP 8.2(a).	KPMG restates the position outlined in our Issues Paper and Discussion Paper submissions supporting the introduction of a mechanism to prescribe countries and certification schemes: • The effectiveness of the APP 8.2(a) and (b) exceptions raise some challenges. In order to rely on these exceptions, an entity must undertake an assessment of the protections afforded by a jurisdiction in which the overseas recipient is located, and such an undertaking can be extremely burdensome on the entity (and potentially duplicates work done by similar entities). • Australia does not currently provide any certainty through an equivalency mechanism or process that recognises the adequacy of overseas privacy laws that are similar to the European Commission's adequacy decision making process for GDPR. This can result in an ad-hoc approach to reliance on the jurisdiction exception or it is otherwise considered as part of the APP 8.1 assessment. • We suggest that APP 8.2 exceptions and how they can effectively support cross-border transfers as part of the scheme should be given further consideration. In particular, an equivalency mechanism similar to the adequacy mechanism under GDPR would provide certainty and reduce burdens on business, without introducing any impact on individuals. • Additionally, existing 'follow-the-sun' support models mean technology platforms utilise global support teams to provide 24-hour service. As a result, personal information may well be accessed or transferred through a number of jurisdictions. There is certainly an opportunity to review and consider ways in which organisations can provide greater confidence to individuals that their information is being handled in a consistent manner. KPMG recognises that a mechanism to prescribe countries and certification schemes as providing substantially similar protections will provide more efficiency in a global market, however there is a risk that countries in emerging markets and not prescribed may be excluded based on their status.
Proposal 23.3 Standard contractual clauses for use when transferring personal information overseas should be made available to APP entities.	KPMG restates the position outlined in our Issues Paper and Discussion Paper submissions supporting the adoption of a model similar to the European Union's Standard Contractual Clauses (SCC) model that is fit for purpose in Australia, which includes standard binding terms that entities can enter into with overseas recipients on the basis of which data transfers would be permitted. In adopting this model, it is important to give individuals appropriate rights and ensure that

	personal information is handled consistently with the APPs and applicable codes.
Proposal 23.4 Strengthen the informed consent exception to APP 8.1 by requiring entities to consider the risks of an overseas disclosure and to inform individuals that privacy protections may not apply to their information if they consent to the disclosure.	KPMG restates the position outlined in our Issues Paper and Discussion Paper submissions supporting the proposal to strengthen the informed consent exception. The requirements for obtaining valid consent for the purposes of relying on 8.2(b) means its application is potentially very limited save in some very specific cases, otherwise the validity of the consent is uncertain.
Proposal 23.5 Strengthen APP 5 in relation to overseas disclosures by requiring APP entities, when specifying the countries in which recipients are likely to be located if practicable, to also specify the types of personal information that may be disclosed to recipients located overseas.	KPMG refers to its comments in Section 10 of this response.
Proposal 23.6 Introduce a definition of 'disclosure' that is consistent with the current definition in APP Guidelines. Further consideration should be given to whether online publications of personal information should be excluded from the requirements of APP 8 where it is in the public interest.	KPMG supports the proposal to include a definition of 'disclosure' to clarify its scope and specifically its application to personal information that is processed or accessed by Cloud Service Providers and other recipients located overseas. The scope of the proposed definition will require careful drafting to avoid greater ambiguity and to the distinction between 'use' and 'disclosure', or too narrowly define what a 'disclosure' consists of.
23. CBPR and domestic certification	No KPMG comment.
24. Enforcement	No KPMG comment.
25. A direct right of action	
Proposal 26.1 Amend the Act to allow for a direct right of action in order to permit individuals to apply to the courts for relief in relation to an interference with privacy. The model should incorporate the appropriate design elements discussed in this chapter.	No KPMG comment.
26. A statutory tort for serious invasions of privacy	
Proposal 27.1 Introduce a statutory tort for serious invasions of privacy in the form recommended by the ALRC in Report 123. Consult with the states and territories on implementation to ensure a consistent national approach.	No KPMG comment.
27. Notifiable data breaches scheme	
Proposal 28.1 Undertake further work to better facilitate the reporting processes for notifiable data breaches to assist both the OAIC and entities with multiple reporting obligations.	KPMG broadly supports this proposal given the reporting burden on entities with multiple reporting obligations. However, we would welcome additional guidance on the extent of information required to be provided in a data breach report in

	circumstances where the reporting requirement is time sensitive, particularly where entities are aware of a suspected, but have not confirmed that an eligible data breach has in fact occurred. Ensuring that individuals are given timely and meaningful information about how to mitigate any harm to them from a breach will also be important.
Proposal 28.2 a) Amend paragraph 26WK(2)(b) to provide that if an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of the entity, the entity must give a copy of the statement to the Commissioner as soon as practicable and not later than 72 hours after the entity becomes so aware, with an allowance for further information to be provided to the OAIC if it is not available within the 72 hours. b) Amend subsection 26WL(3) to provide that if an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of an entity the entity must notify the individuals to whom the information relates as soon as practicable and where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases as soon as practicable. c) Require entities to take reasonable steps to implement practices, procedures and systems to enable it to respond to a data breach.	KPMG broadly supports this proposal, but would welcome additional guidance on what would constitute 'reasonable grounds' which would trigger the 72-hour reporting period, and how this requirement would interact with the 30-day assessment period that commences after an entity has reasonable grounds to suspect an eligible data breach may have occurred. Commentary around this proposal appears to suggest that its purpose is to align data breach reporting timeframes to that of the GDPR, however should the period to assess a suspected eligible data breach under s26WH(2) of the Act (up to 30 days) remain, there does not appear to be a material change in the time an affected individual would be notified of a breach. KPMG would welcome guidance on whether the proposal is aiming to encourage 'precautionary notifications'. This is an increasingly common practice whereby entities notify affected individuals of basic details of a suspected eligible data breach as soon as practicable after becoming aware of the breach (including precautions they can take, e.g. to monitor their accounts for scams), despite not being in a position to confirm, for each individual, whether the circumstances of the breach would be likely to cause them serious harm and in order potentially to support remediation of a data breach. KPMG considers it would be a beneficial practice to encourage early notification of breaches, though acknowledges that careful balance is required to reduce burden from over-notification.
Proposal 28.3 Amend subsections 26WK(3) and 26WR(4) to the effect that a statement about an eligible data breach must set out the steps the entity has taken or intends to take in response to the breach, including, where appropriate, steps to reduce any adverse impacts on the individuals to whom the relevant information relates. However, this proposal would not require the entity to reveal personal information, or where the harm in providing this information would outweigh the benefit in providing this information. Consider further a requirement that entities should take reasonable steps to prevent or reduce the harm that is likely to arise for individuals as a result of a data breach.	KPMG supports this proposal, subject to supplementary guidance being developed that would assist entities in determining the steps they should take in response to a breach that is proportionate to the adverse impacts on the individuals. KPMG observes that there is currently little information available to entities to help them understand (practically) how to remediate harm from a breach. KPMG considers that there may be a role for a 'best practice' remediation template to be developed in consultation with industry and technical security and other bodies. KPMG would welcome guidance on the improvement of technical controls to support breach prevention and protection as a direct consequence of the Notifiable Data Breaches Scheme, which is an area we consider entities should be encouraged to also focus on.

Proposal 28.4 Introduce a provision in the Privacy Act to enable the Attorney-General to permit the sharing of information with appropriate entities to reduce the risk of harm in the event of an eligible data breach. The provision would contain safeguards to ensure that only limited information could be made available for designated purposes, and for a time limited duration.	KPMG agrees in principle with this proposal subject to understanding more about the safeguards, and to what extent entities will be given guidance on how the safeguards would apply to them practically. KPMG would also support minimum technical/security standards on the method of transfer of information to prevent any inadvertent additional risk to individual's information from such transfer.
28. Interactions with other schemes	
Proposal 29.1 The Attorney-General's Department develop a privacy law design guide to support Commonwealth agencies when developing new schemes with privacy-related obligations.	KPMG supports these proposals which aim to address interactions with the broader landscape of data-related regulatory requirements at a state and federal level. We encourage collaboration between Commonwealth agencies to ensure harmonisation between overlapping regulatory frameworks.
Proposal 29.2 Encourage regulators to continue to foster regulatory cooperation in enforcing matters involving mishandling of personal information.	
Proposal 29.3 Establish a Commonwealth, state and territory working group to harmonise privacy laws, focusing on key issues.	
30. Further review	
Proposal 30.1 Conduct a statutory review of any amendments to the Act which implement the proposals in this Report within three years of the date of commencement of those amendments.	KPMG supports this proposal.

Key authors and contacts

Veronica Scott
Partner, Cyber and Privacy Law

Kelly Henney
Partner, Privacy and Data Protection

Linda Chai
Partner, KPMG Enterprise

Jana Katerinskaja
Director, KPMG Privacy Officer

Shubham Singhal
Director, Compliance and Conduct, Privacy and Data Protection

Paola Redecilla
Associate Director, Compliance and Conduct, Privacy and Data Protection

Mark Dunning
Associate Director, Compliance and Conduct, Privacy and Data Protection

David Markus
Associate Director, Compliance and Conduct, Privacy and Data Protection

Rob Griffiths
Manager, Management Consulting

Steph Cosentino
Manager, KPMG Law

Jason Kaye
Manager, KPMG Law

Leah Roy
Manager, Compliance and Conduct, Privacy and Data Protection

Caitlin Galpin
Manager, Compliance and Conduct, Privacy and Data Protection

Naveen Malhotra
Manager, Compliance and Conduct, Privacy and Data Protection

Sid Jujjavarapu
Manager, Compliance and Conduct, Privacy and Data Protection

Joanne Ewen
Senior Consultant, Privacy

Niran Garcha
Senior Consultant, Compliance and Conduct, Privacy and Data Protection

Elly Krambias
Consultant, KPMG Law

Sophie Finemore
Director, Corporate Affairs

Olivia Spurio
Manager, Corporate Affairs

KPMG.com.au