KPMG

REVIEW OF THE PRIVACY ACT 1988

Discussion Paper

KPMG Australia

January 2022

KPMG.com.au

Contents

Executive summary

KPMG Australia (KPMG) welcomes the opportunity to provide a submission to the Attorney-General Department's review of the Privacy Act 1988 (Cth) (the Review). The Review is a significant opportunity to contribute to an important reform process that has the potential to empower consumers and protect their data, while creating economy wide benefits.

As a leading professional services firm, 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 to debate that seeks to develop a strong and prosperous economy and society and welcome the opportunity to provide a submission to the Review.

Entities currently must manage and comply with a range of data-related regulatory requirements that exist in overlapping and in some cases fragmented frameworks at both a State and Federal level. The Review provides a further opportunity to carefully consider how the Privacy Act (the Act) interacts with these frameworks, including the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (the Online Privacy Bill) and the recently passed Security Legislation Amendment (Critical Infrastructure) Bill 2021 (the Critical Infrastructure Bill).

The expansive list of objects outlined in the Act have, in our view, endured well since they were introduced 20 years ago. KPMG supports the continued broad objects of the Act and believes that care should be taken to avoid narrowing, even unintentionally, the objects 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.

The Discussion Paper opens the way for potential wide-ranging reforms of the Act and beyond. KPMG considers that greater clarity about the objectives of the reform should be a primary consideration of the Review. KPMG therefore believes that clear articulation of the problem statement for the proposed changes will be critical to drive a clear and comprehensive framework for reform of the Act, that builds on and strengthens the core principles-based elements of the Act, provides clarity and accountability for entities, and enhances individual rights while not overburdening them as the central modern privacy law for Australia.

This submission builds on KPMG's submission to the Review's Issues Paper[1]. It outlines 26 findings at section one and directly addresses the complete list of proposals at section two. KPMG looks forward to continued engagement as this important review process progresses.

Yours sincerely,

Kate Marshall
Head of KPMG Law
KPMG Australia

Kelly Henney
Compliance & Conduct Leader, Privacy & Data Protection
KPMG Australia

Mark Tims
Head of Technology Risk & Cyber Security
KPMG Australia

[1] https://home.kpmg/au/en/home/insights/2021/01/review-privacy-act-1988-cth-kpmg-issues-paper.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 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 pull together a comprehensive response to a complex area of law.

Section 1: KPMG findings

FINDING 1

KPMG considers that greater clarity about the objectives of the reform and how these will be achieved should be a primary consideration of the Review. This could be achieved by the articulation of a problem statement.

FINDING 2:

The Review should seek to undertake a rigorous Regulatory Impact Statement to assess costs and benefits of multiple reform options.

FINDING 3:

KPMG supports the proposed addition of "with regard to their personal information" outlined at 1.1 (a) in order to clarify that the Act's scope relates specifically to information privacy.

FINDING 4:

KPMG considers the proposed addition of "undertaken in the public interest" at 1.1 (b) may require further consideration and refinement in order to avoid unduly narrowing an entity's legitimate purposes and objectives. Public interest could instead be a separate basis for lawful processing, including in relation to special types of personal information.

FINDING 5:

KPMG supports preserving rather than amending the current definition of personal information and suggests instead that the existing guidance and APP Code-making powers in the Act could be better utilised to provide more clarity about what personal information is, and address industry-specific concerns and specific privacy risks.

FINDING 6:

KPMG suggests a cautious approach to re-introducing the Privacy Amendment (Re-identification) Office Bill given the potential for unintended consequences. Greater clarity around the intended objective in the context of the overall reforms and careful consideration of potential flow on effects and how this relates to other proposed amendments would be important.

FINDING 7:

KPMG considers that APP code-making powers in the Act are a better way of addressing discrete issues rather than making wholesale changes to the Act, though caution should be taken to ensure any measure with legislative power goes through proper and appropriate review processes.

FINDING 8:

KPMG considers that there should be no change to the current threshold for notice requirements which is effective and sufficiently flexible, that information relating to cross-border disclosure of personal information and whether the collection is required or authorised by law/a court order should be kept, and the period for which the information collected will be stored should be added into privacy notices.

FINDING 9:

The Review should assess how to make notices more effective in practice, in a way that strikes the right balance to avoid notification fatigue, drive timely and meaningful notification and empower consumers, while maintaining flexibility.

FINDING 10:

The use of consent as an effective default lawful basis for collecting and processing personal information should be reviewed in the context of the development of technology, the use of data surveillance, cloud computing and increasingly data driven business and government.

FINDING 11:

KPMG considers that the requirement for consent to be 'freely given' could be added. However, this would require an alternative lawful basis, such as legitimate interest. It may also be worthwhile to include guidelines which specify a time period where consent renewal may be needed.

FINDING 12:

In relation to pro-privacy default settings outlined at proposal 12.1, KPMG considers Option 2 would be preferable as it allows users to fully understand their privacy options and promotes implementation of more restrictive privacy settings. However, should Option 2 be adopted, KPMG considers that it would have to be managed in a way that does not cause undue user frustration, similar to Cookie banners, as seen within Europe.

FINDING 13:

KPMG considers that further clarity should be provided on how the age of 16 has been determined as the appropriate assumed age of capacity for exercising privacy rights or providing consent. Consideration could also be given to introducing the concept of a 'mature minor'.

FINDING 14:

The Review could consider how proposal 14.1 works with the Online Privacy Code where individuals can ask for their information. There should also be consideration given to whether in addition to the right, legitimate interest could override objection or withdrawal of consent.

FINDING 15:

KPMG considers that there may not be an apparent need to introduce a specific right to erasure, as current data rights and regulatory powers of the Information Commissioner require personal information to be deleted in appropriate circumstances.

FINDING 16:

KPMG considers that APP 7 should not be removed unless appropriate protections and rights are introduced including the primary right to object.

FINDING 17:

KPMG supports the proposed option 17.1 on automated decision-making. Where personal information will be used in automated decision making, KPMG considers that it should be transparent and there should be an option to opt out from personal information being used in this way.

FINDING 18:

In KPMG's view the requirements placed on entities to destroy or de-identify personal information are appropriate and balanced.

FINDING 19:

When processing personal information, KPMG supports proposal 19.3 that APP entities should take all reasonable steps to destroy or anonymise information where the entity no longer needs the information for any purpose for which the information may be used or disclosed according to the APPs.

FINDING 20:

KPMG supports proposal 20.1 to introduce further organisational accountability requirements into the Act, including the amendment of APP 6 as outlined at 20.1. The amendment of additional APPs could also be considered to further increase organisational accountability under the Act.

FINDING 21:

KPMG considers that an equivalency mechanism similar to the adequacy mechanism under GDPR would provide certainty and reduce burdens on business, without introducing any impact on individuals.

FINDING 22:

Any further take-up or endorsement of the CBPR should be carefully considered in the context of the overall objective and net benefits as well as the frameworks established by the reformed Act.

FINDING 23:

In KPMG's view there is a potential risk of additional burden on entities that must respond to multiple regulators on essentially similar matters, as well as confusion for consumers, and this overlap should be carefully considered as part of the Review. The establishment of a centralised Federal Privacy Ombudsman (Option 2) to support and strengthen privacy enforcement may alleviate this.

FINDING 24:

When considering enforcement options, KPMG recommends consideration of which regulatory model will have the capacity, resources and appetite to best enforce regulation or issue penalties.

FINDING 25:

KPMG submits that careful consideration should be given to inserting a direct right of action in the Act. In our view it would not be the most appropriate mechanism to include in the context of how the regulatory framework operates.

FINDING 26:

KPMG considers that a statutory tort of privacy would not be the most appropriate mechanism to introduce in the Act in any form, whether in relation to private sector entities or individuals in a non-business capacity.

.

Section 2: KPMG insights

The Privacy Act underwent major reform in 2014 (with the introduction of the APPs and the comprehensive credit reporting regime) and again in 2018 (with the introduction of the Notifiable Data Breaches (NDB) Scheme). Since then, the role of technology and data in the economy and the international flows of data in society have continued to change and accelerate.

As outlined in KPMG's submission to the Issues Paper[2], there are several factors that make this Review important and timely and require us to think about what the purpose, processes and outcomes of reform should be. Furthermore, privacy and consumer rights are converging and new cyber, digital and data laws are being developed, both in Australia and overseas. It is in this complex and dynamic environment that the Review must proceed, and therefore the Review of the Act must be undertaken with care and caution.

For example, consultation is currently underway on the Online Privacy Bill. While KPMG does not intend to respond directly to this process, we consider that it would be worthwhile completing the Review of the Act before making changes to the Online Privacy Bill given the areas of overlap that exist between these two pieces of legislation and ensuring that the Privacy Act remains the central privacy law.

The Discussion Paper opens the way for potential wide-ranging reforms of the Act and beyond, and KPMG considers that greater clarity about the objectives of the reform should be a primary consideration of the Review.

To this end, KPMG believes that adequate articulation of the problem statement for the proposed changes will be critical in ensuring that reforms will appropriately address the problem and result in consumer benefit as well as additional clarity for entities. It will also be important to consider any potential flow on or unintended effects of any changes made in a comprehensive Regulatory Impact Statement (RIS).

As outlined in our submission to the Issues Paper, the development of a regulatory framework that is responsive to the rights of individuals and needs of entities in the Australian context should in our view be the primary objective. This could be clearly articulated by committing to undertake a rigorous RIS process that would assess costs and benefits of multiple reform options.

KPMG has responded directly to the Discussion Paper's complete list of proposals in the section below.

FINDING 1: KPMG considers that greater clarity about the objectives of the reform and how these will be achieved should be a primary consideration of the Review. This could be achieved by the articulation of a problem statement.

FINDING 2: The Review should seek to undertake a rigorous Regulatory Impact Statement to assess costs and benefits of multiple reform options.

[2] https://assets.kpmg/content/dam/kpmg/au/pdf/2021/kpmg-issues-paper-review-of-the-privacy-act-1988.pdf

Response to Discussion Paper – Complete list of proposals

Part 1: Scope and application of the Act

1. Objects of the Act

1.1. Amend the objects in section 2A, to clarify the Act's scope and introduce the concept of public interest, as follows:

(a) to promote the protection of the privacy of individuals *with regard to their personal information*, and

(b) to recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities *undertaken in the public interest*.

KPMG response

The expansive list of objects outlined in section 2A of the Act have, in our view, endured well since they were introduced 20 years ago. KPMG supports the continued broad objects of the Act and considers that care should be taken to avoid narrowing, even unintentionally, the objects in an attempt to address perceived limitations in the Discussion Paper. 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 any Regulatory Impact Statement process.

We support the proposed addition outlined at 1.1 (a) in order to clarify that the Act's scope relates specifically to information privacy, i.e. an individual's personal information, and not more general common conceptions of privacy such as physical privacy or personal space. This qualification exists in practice in interpreting and complying with the Act, however the amendment would assist to make the scope more explicit for those not so familiar with the Act. KPMG considers it may also be beneficial amending the wording of *with regard to* and replacing it with *in relation to*.

In KPMG's view, the proposed addition in 1.1 (b) may require further consideration and refinement. We recognise that the rationale for its addition is to ensure an entity does not over-emphasise their own commercial objectives in striking the right balance. However, an entity's legitimate purposes and objectives, particularly many private sector APP entities, may not always be considered to be in the public interest as that term is generally understood, given the nature of their commercial operations. This could severely limit their ability to process personal information which would ultimately have broad benefits to the community and economy in, for example, providing goods and services, generating jobs and revenue.

Public interest could instead be a separate basis for lawful processing, including in relation to special types of personal information, which is the approach adopted in other privacy legislation such as the European Union's General Data Protection Regulation (GDPR).

The amendment could otherwise also be misinterpreted to mean this balance only needs to be considered when acting on public interest matters rather than broader commercial operations. KPMG also considers that as an alternative, the insertion of *legitimate functions or activities* would assist in ensuring the right balance.

We believe consideration should also be given to how *public interest* would be interpreted, and how smaller businesses, who aren't exempt, would assess this. It could potentially add to regulatory burden without clear benefits.

Additionally, it is our view that for greater consistency the proposed amendment in 1.1 (a) could be replicated in 1.1 (b) following the reference to *privacy of individuals*.

FINDING 3: KPMG supports the proposed addition of "with regard to their personal information" outlined at 1.1 (a) in order to clarify that the Act's scope relates specifically to information privacy.

FINDING 4: KPMG considers the proposed addition of "undertaken in the public interest" at 1.1 (b) may require further consideration and refinement in order to avoid unduly narrowing an entity's legitimate purposes and objectives. Public interest could instead be a separate basis for lawful processing, including in relation to special types of personal information.

2. Definition of personal information

2.1. Change the word 'about' in the definition of personal information to 'relates to'.

2.2. Include a non-exhaustive list of the types of information capable of being covered by the definition of personal information.

2.3. Define 'reasonably identifiable' to cover circumstances in which an individual could be identified, directly or indirectly. Include a list of factors to support this assessment.

2.4. Amend the definition of 'collection' to expressly cover information obtained from any source and by any means, including inferred or generated information.

2.5. Require personal information to be anonymous before it is no longer protected by the Act.

2.6. Re-introduce the Privacy Amendment (Re-identification) Offence Bill 2016 with appropriate amendments.

KPMG response

The Act regulates personal information, and the definition determines the breadth of what data is regulated. Any changes should be carefully considered. As per our submission to the Issues Paper, KPMG supports preserving rather than amending the current definition and suggests instead that the existing guidance and APP Code-making powers in the Act could be better utilised to provide more clarity about what personal information is, including in relation to technical information, and address industry-specific concerns and specific privacy risks that may require specific protections.

As per KPMG's submission to the Issues Paper, clarity about the concept of 'anonymised' information and how it may be better protected or governed under industry-specific codes should be the subject of further guidance which also allows flexibility to evolve. Any attempt to enshrine in legislation an industry-accepted technical standard of de-identification or anonymisation should be resisted.

In relation to proposal 2.6, *re-introduce the Privacy Amendment (Re-identification) Offence Bill 2016 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. Furthermore, as per Finding 1, 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'.

FINDING 5: KPMG supports preserving rather than amending the current definition of personal information and suggests instead that the existing guidance and APP Code-making powers in the Act could be better utilised to provide more clarity about what personal information is, and address industry-specific concerns and specific privacy risks.

FINDING 6: KPMG suggests a cautious approach to re-introducing the Privacy Amendment (Re-identification) Office Bill given the potential for unintended consequences. Greater clarity around the intended objective in the context of the overall reforms and careful consideration of potential flow on effects and how this relates to other proposed amendments would be important.

3. Flexibility of the APPs

3.1. Amend the Act to allow the Information Commissioner (IC) to make an APP code on the direction or approval of the Attorney General:

– where it is in the public interest to do so without first having to seek an industry code developer, and

– where there is unlikely to be an appropriate industry representative to develop the code

3.2. Amend the Act to allow the IC to issue a temporary APP code on the direction or approval of the Attorney-General if it is urgently required and where it is in the public interest to do so.

3.3. Amend Part VIA of the Act to allow 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.

3.4. Amend the Act to permit organisations to disclose personal information to state and territory authorities when an Emergency Declaration is in force.

KPMG response

As stated previously, KPMG considers that APP code-making powers in the Act are a better way of addressing discrete issues rather than making wholesale changes to the Act. Caution should be taken in order to ensure any measure with legislative power behind it goes through proper and appropriate review processes. It is our view that consideration should be given to what the problem is that these proposals are seeking to address, and it may be worthwhile considering the purpose of APP codes and seeking feedback on how they are being used and if they can be employed more effectively.

FINDING 7: KPMG considers that APP code-making powers in the Act are a better way of addressing discrete issues rather than making wholesale changes to the Act, though caution should be taken to ensure any measure with legislative power goes through proper and appropriate review processes.

Part 2: Protection

8. Notice of collection of personal information

8.1. Introduce an express requirement in APP 5 that privacy notices must be clear, current and understandable.

8.2. APP 5 notices limited to the following matters under APP 5.2:

- the identity and contact details of the entity collecting the personal information
- the types of personal information collected
- the purpose(s) for which the entity is collecting and may use or disclose the personal information
- the types of third parties to whom the entity may disclose the personal information
- if the collection occurred via a third party, the entity from which the personal information was received and the circumstances of that collection
- the fact that the individual may complain or lodge a privacy request (access, correction, objection or erasure), and

8.3. the location of the entity's privacy policy which sets out further information. Standardised privacy notices could be considered in the development of an APP code, such as the OP code, including standardised layouts, wording and icons. Consumer comprehension testing would be beneficial to ensure the effectiveness of the standardised notices.

8.4. Strengthen the requirement for when an APP 5 collection notice is required – that is, require notification at or before the time of collection, or if that is not practicable as soon as possible after collection, unless:

- the individual has already been made aware of the APP 5 matters; or
- notification would be impossible or would involve disproportionate effort.

KPMG response

KPMG considers that current notice requirements relating to any cross-border disclosure of personal information and disclosing whether the collection is required or authorised by law should remain (see APP5.2 (c) and (i)), and supports adding the period for which the information will be stored into privacy notices. Additionally, we support point 8.3 in relation to standardised privacy notices as per our submission to the Issues Paper which highlighted that this kind of standardisation would enhance user experience and help users make informed decisions.

As per KPMG's submission to the Issues Paper, we also note the following:

Improving awareness of relevant matters

Consistent with the objects of the Act, the current approach to collection in APPs 3 and 5 allows APP entities to balance the protection of the privacy of individuals with their own interests in carrying out their functions or activities and should remain unaltered. This approach has meant that there are now more opportunities to more closely scrutinise the notice provided to ensure that the purposes of collection, use and disclosure are clear and adhered to by the APP entity.

KPMG does not support changing the current threshold test as proposed in 8.4 from the requirement to take 'such steps (if any) as reasonable in the circumstances' which we consider would have a material impact on and undermine the current flexibility. This requires consideration of all the circumstances and the possibility that individuals are already aware of some or all of the matters already. There are many situations where notice may not be impossible or have disproportionate effort, but this would not achieve the right balance outlined above. The current test considers the particular context of the collection, and prevents additional burden and notification on individuals where they are already aware of some of the relevant matters. Further, the APP Guidelines to APP 5 outline the circumstances when it may not be reasonable to provide a notice.

Third party collections

In considering how the current system responds to the concept of indirect collection, notice needs to remain practicable and the current system correctly 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 inform the individual of any indirect collection or potential transfer of data to a third party. Broadening the requirements to provide notice across a data supply chain over and above that original notice would lead to a greater burden on individuals as well as notice fatigue, in receiving, reviewing, digesting and consenting to privacy notices.

The following new proposed requirement for privacy notices is, in our view, a more effective mechanism: where collection occurred via a third party, the first party must disclose the entity from which the personal information was received and the circumstances of that collection.

Limiting information burden on individuals

Consistent with the objects of the Act, the current approach to collection in APPs 3 and 5 allows APP entities to balance the protection of the privacy of individuals with their own interests in carrying out their functions or activities and should remain unaltered. This approach has meant that there are now more opportunities to more closely scrutinise the notice provided to ensure that the purposes of collection, use and disclosure are clear and adhered to by the APP entity.

FINDING 8: KPMG considers that there should be no change to the current threshold for notice requirements which is effective and sufficiently flexible, that information relating to cross-border disclosure of personal information and whether the collection is required or authorised by law/a court order should be kept, and the period for which the information collected will be stored should be added into privacy notices.

FINDING 9: The Review should assess how to make notices more effective in practice, in a way that strikes the right balance to avoid notification fatigue, drive timely and meaningful notification and empower consumers, while maintaining flexibility.

9. Consent to the collection, use and disclosure of personal information

9.1. Consent to be defined in the Act as being voluntary, informed, current, specific, and an unambiguous indication through clear action.

9.2. Standardised consents could be considered in the development of an APP code, such as the OP code, including standardised layouts, wording, icons or consent taxonomies. Consumer comprehension testing would be beneficial to ensure the effectiveness of the standardised consents.

KPMG response

Consent is increasingly relied on as a basis for the lawful collection, use and disclosure of personal information. The use of consent as the default lawful basis for collecting and processing personal information should be reviewed in the context of the development of technology, the use of data surveillance, cloud computing and increasingly data driven business and government.

Obtaining meaningful and lawful consent in relation to the processing of all types of personal information is not always possible or practical and places the onus on individuals. The Review should also investigate alternatives to consent as a means for lawfully processing personal information, such as legitimate interests, in a manner that does not compromise privacy protections and reflects other proposed requirements such assessing high impact activities, accountability and the right to object.

In relation to the proposals at section nine, KPMG considers that in addition to the elements of consent defined at 9.1, the requirement for consent to be 'freely given' could be added. However, this would require an alternative lawful basis, such as legitimate interest. It may also be worthwhile to include consent refresh guidelines which specify circumstances or a time period where consent refresh or renewal may be needed.

Commissioner guidelines would also assist in further clarity of the consent requirements, for example:

- 'Specified' meaning unbundled;
- Define 'current', i.e. consent refresh or renewal when required;
- 'Clear action' meaning no pre-ticked boxes; and
- Limited use of opt-out consent, e.g. certain direct marketing where it is related to the initial product/service.

Several other issues for consideration by the Review include guidance on child consent, the potential to require a consent assessment test to determine if it is the most appropriate approach (such as the Legitimate Interests Assessment (LIA) approach outlined by the ICO in relation to the UK GDPR), and seeking to develop a common language around data and consent, including for vulnerable people and children. The Online Privacy Bill also addresses these matters.

As per KPMG's submission to the Issues Paper, any amendments must ensure that the regulatory burden is not disproportionate, with a focus on effective and meaningful disclosure through notices at or before the time of collection to enable valid consent to be provided.

FINDING 10: The use of consent as an effective default lawful basis for collecting and processing personal information should be reviewed in the context of the development of technology, the use of data surveillance, cloud computing and increasingly data driven business and government.

FINDING 11: KPMG considers that the requirement for consent to be 'freely given' could be added. However, this would require an alternative lawful basis, such as legitimate interest. It may also be worthwhile to include guidelines which specify a time period where consent renewal may be needed.

10. Additional protections for collection, use and disclosure of personal information

10.1. A collection, use or disclosure of personal information under APP 3 and APP 6 must be fair and reasonable in the circumstances.

10.2. Legislated factors relevant to whether a collection, use or disclosure of personal information is fair and reasonable in the circumstances could include:

- Whether an individual would reasonably expect the personal information to be collected, used or disclosed in the circumstances
- The sensitivity and amount of personal information being collected, used or disclosed
- Whether an individual is at foreseeable risk of unjustified adverse impacts or harm as a result of the collection, use or disclosure of their personal information
- Whether the collection, use or disclosure is reasonably necessary to achieve the functions and activities of the entity
- Whether the individual's loss of privacy is proportionate to the benefits
- The transparency of the collection, use or disclosure of the personal information, and
- 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.

10.3. Include an additional requirement in APP 3.6 to the effect that 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.

10.4. Commissioner-issued guidelines could provide examples of reasonable steps that could be taken, including making reasonable enquiries regarding the collecting entities' notice and consent procedures or seeking contractual warranties that the information was collected in accordance with APP 3.

10.5. Define a 'primary purpose' as the purpose for the original collection, as notified to the individual. Define a 'secondary purpose' as a purpose that is directly related to, and reasonably necessary to support the primary purpose.

KPMG response

The current requirements in APP 3 are that APP entities must only collect personal information that is reasonably necessary for their functions and activities and collection must also be only by fair and lawful means.

The replacement of these requirements with a fair and reasonable threshold requirement for APP 3 and the addition of this requirement in APP 6 imposes additional privacy protections which reflect good practice and community expectations. 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 having regard to our response to the proposed amendment to the Objects of the Act in section 1.1 (b).

In relation to the proposed list of legislated factors at 10.2, KMPG considers that it is better for guidance to be provided and that the list should not be exhaustive. Further clarity should also be provided about where disclosure is required or authorised by law.

The proposal to limit secondary purpose to being defined as that which 'directly relates to' and is 'reasonably necessary to support' the primary purpose, substantially limits the secondary purposes for which personal information may be permitted to be used or disclosed. This would have a significant impact on organisations' ability to process personal information in accordance with applicable exceptions in the absence of an alternative basis such as legitimate interest.

Furthermore, proposal 10.3 does not appear to take into account insights derived from or inferred from personal information that has already been collected.

11. Restricted and prohibited acts and practices

11.1. **Option 1** – APP entities that engage in the following restricted practices must take reasonable steps to identify privacy risks and implement measures to mitigate those risks:

- Direct marketing, including online targeted advertising on a large scale
- The collection, use or disclosure of sensitive information on a large scale
- The collection, use or disclosure of children's personal information on a large scale
- The collection, use or disclosure of location data on a large scale
- The collection, use or disclosure of biometric or genetic data, including the use of facial recognition software
- The sale of personal information on a large scale
- The collection, use or disclosure of personal information for the purposes of influencing individuals' behaviour or decisions on a large scale

- The collection use or disclosure of personal information for the purposes of automated decision making with legal or significant effects, or
- Any collection, use or disclosure that is likely to result in a high privacy risk or risk of harm to an individual.

11.2. **Option 2** – In relation to the specified restricted practices, increase an individual's capacity to self-manage their privacy in relation to that practice.

Possible measures include consent (by expanding the definition of sensitive information), granting absolute opt-out rights in relation to restricted practices (see Chapter 14), or by ensuring that explicit notice for restricted practices is mandatory.

KPMG response

In relation to Option 1, KPMG suggests that these matters should be considered in the context of the overarching privacy by design obligations in APP 1. They should reflect the steps involved in, and the purpose of, for example, a Privacy Impact Assessment which is referred to in the Office of the Australian Information Commissioner's (OAIC) APP 1 Guidelines as an example of privacy by design.

Further and related to this, as per our response to section three, 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. As per Finding 7, KPMG considers that caution should be taken to ensure anything with legislative power goes through proper and appropriate review processes.

12. Pro-privacy default settings

12.1. Introduce pro-privacy defaults on a sectoral or other specified basis.

- **Option 1** – Pro-privacy settings enabled by default: Where an entity offers a product or service that contains multiple levels of privacy settings, an entity must pre-select those privacy settings to be the most restrictive. This could apply to personal information handling that is not strictly necessary for the provision of the service, or specific practices identified through further consultation.
- **Option 2** – Require easily accessible privacy settings: Entities must provide individuals with an obvious and clear way to set all privacy controls to the most restrictive, such as through a single click mechanism.

KPMG response

In relation to pro-privacy default settings, we consider that Option 2 would be preferable. Option 2 requires easily accessible privacy settings: *Entities must provide individuals with an obvious and clear way to set all privacy controls to the most restrictive, such as through a single click mechanism*. This option would allow users to fully understand their privacy options should they wish to and promotes implementing further privacy settings. Should Option 2 be adopted, KPMG considers that it would have to be managed in a way that does not cause undue user frustration, similar to Cookie banners, as seen within Europe.

While Option 1 carries benefits such as the data subject inherently being provided a service that impedes the least on their privacy rights and freedoms without having to think about it or change settings, KPMG considers that there are a number of factors that should be considered. Should Option 1 be adopted, entities may choose not to offer any further privacy settings than what is required by the Act and could therefore be counterintuitive to overall benefit to consumer privacy.

Furthermore, as noted above regarding Option 2, if the most restrictive privacy settings also included cookie settings, it could reduce the user experience of the services being provided.

Finally, KPMG considers that enhancement of privacy by design obligations (in APP 1) would also assist as it would require entities to consider these matters.

FINDING 12: In relation to pro-privacy default settings outlined at proposal 12.1, KPMG considers Option 2 would be preferable as it allows users to fully understand their privacy options and promotes implementation of more restrictive privacy settings. However, should Option 2 be adopted, KPMG considers that it would have to be managed in a way that does not cause undue user frustration, similar to Cookie banners, as seen within Europe.

13. Children and vulnerable individuals

13.1. Amend the Act to require consent to be provided by a parent or guardian where a child is under the age of 16. The Review is seeking additional feedback on whether APP entities should be permitted to assess capacity on an individualised basis where it is practical to do so. The Review is also seeking feedback on the circumstances in which parent or guardian consent must be obtained:

- **Option 1** – Parent or guardian consent to be required before collecting, using or disclosing personal information of the child under the age of 16.
- **Option 2** – In situations where the Act currently requires consent, including before the collection of sensitive information or as an available mechanism to undertake a secondary use or disclosure of personal information.

The assumed age of capacity would also determine when a child may exercise privacy requests independently of their parents, including access, correction or erasure requests.

13.2. Require APP 5 notices to be clear, current and understandable, *in particular for any information addressed specifically to a child*.

KPMG response

KPMG considers that further clarity should be provided on how the age of 16 has been determined as the appropriate and persistent assumed age of capacity for exercising privacy rights or providing consent. The Review could consider whether 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.

Consideration could be given to introducing the concept of a 'mature minor', where a young person may be sufficiently mature and capable of making their own decision. The Office of the Victorian Information Commissioner (OVIC) refers to competence: *A minor is, according to this principle, capable of giving informed consent when he or she "achieves a sufficient understanding or intelligence to enable him or her to understand fully what is proposed"*.

Additionally, when considering legislation regarding children and vulnerable individuals it would be beneficial to ensure consistency with the Online Privacy code, which requires reasonable steps to verify age, and the requirement to obtain consent from parents for children under 16 years of age before collecting personal information.

FINDING 13: KPMG considers that further clarity should be provided on how the age of 16 has been determined as the appropriate assumed age of capacity for exercising privacy rights or providing consent. Consideration could also be given to introducing the concept of a 'mature minor'.

14. Right to object and portability

14.1. An individual may object or withdraw their consent at any time to the collection, use or disclosure of their personal information.

On receiving notice of an objection, an entity must take reasonable steps to stop collecting, using or disclosing the individual's personal information and must inform the individual of the consequences of the objection.

KPMG response

The role of consumer choice and control, and the privacy tools that support this principle, is an important one that should be considered 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 in our view help to enhance the interests of individuals in the management and control of their personal information and balance the burden imposed by the reliance on consent. Consideration should be given to any qualifications to the right, having regard to appropriate legitimate bases or interest (separate to processing being dependent on consent which can be withdrawn).

In relation to proposal 14.1, the Review could consider how this proposal works with the Online Privacy code where individuals can ask for their information. There should also be consideration given to whether in addition to the right, there should be an opportunity for the entity or data controller to demonstrate compelling legitimate interest for the processing which could override the interests of the data subject.

FINDING 14: The Review could consider how proposal 14.1 works with the Online Privacy Code where individuals can ask for their information. There should also be consideration given to whether in addition to the right, legitimate interest could override objection or withdrawal of consent.

15. Right to erasure of personal information

15.1. An individual may only request erasure of personal information where one of the following grounds applies, and subject to exceptions:

- the personal information must be destroyed or de-identified under APP 11.2
- the personal information is sensitive information
- an individual has successfully objected to personal information handling through the right to object (see Chapter 14)
- the personal information has been collected, used or disclosed unlawfully
- the entity is required by or under an Australian law, or a court/tribunal order, to destroy the information, and
- the personal information relates to a child and erasure is requested by a child, parent or authorised guardian.

15.2. Provide for exceptions to an individual's right to erasure of personal information. An APP entity could refuse a request to erase personal information to the extent that an exception applied to either all or some of the personal information held by an APP entity.

15.3. An APP entity must respond to an erasure request within a reasonable period. If an APP entity refuses to erase the personal information because an exception applies, the APP entity must give the individual a written notice that sets out the reasons for refusal and mechanisms available to complain about the refusal, unless unreasonable to do so.

KPMG response

KPMG considers that the need to introduce a specific right to erasure should be further considered noting that the introduction of this right in the GDPR was in a different legal context compared to Australia. Currently APP 11.2 requires personal information to be deleted in appropriate circumstances and there is guidance in the APP Guidelines. Additionally, APP 10 and APP 13 respectively impose obligations on entities to take steps to correct personal information, and gives individuals the right to request correction.

The impact of introducing a specific right to erasure on a range of other interests, freedoms, rights and law enforcement activities would need to be carefully assessed and the perimeter of the right clearly defined, and consideration should be given to enhancing APPs 10, 11.2 and 13 through amendment or guidance, rather than introduction of entirely new obligations. The right would also place the burden on the individual to request deletion of their personal information in circumstances where there would be a positive obligation on the entity to not process and/or destroy the information in the examples given. The focus should instead be on how to ensure entities are complying with their obligations.

Similar to the right to erasure for an individual who has successfully objected to personal information handling, consideration should also be given to affording the right to erasure to an individual who successfully withdraws their consent (subject to exceptions). However, consent would need to be 'freely given' in order to fulfil the request in many instances.

If this option is to be adopted, further guidance should be provided to quantify 'within a reasonable period'. Additionally, consideration should be given to specifying a time period by which the request should generally be fulfilled and only exceeded by exception.

FINDING 15: KPMG considers that there may not be an apparent need to introduce a specific right to erasure, as current data rights and regulatory powers of the Information Commissioner require personal information to be deleted in appropriate circumstances.

16. Direct marketing, targeted advertising and profiling

16.1. The right to object, discussed at Chapter 14, would include an unqualified right to object to any collection, use or disclosure of personal information by an organisation for the purpose of direct marketing. An individual could still request not to receive direct marketing communications from an organisation. If an organisation provides marketing materials to an individual, it must notify the individual of their right to object in relation to each marketing product provided.

On receiving notice of an objection, an entity must stop collecting, using or disclosing the individual's personal information for the purpose of direct marketing and must inform the individual of the consequences of the objection.

16.2. The use or disclosure of personal information for the purpose of influencing an individual's behaviour or decisions must be a primary purpose notified to the individual when their personal information is collected.

16.3. APP entities would be required to include the following additional information in their privacy policy:

– whether the entity is likely to use personal information, alone or in combination with any other information, for the purpose of influencing an individual's behaviour or decisions and if so, the types of information that will be used, generated or inferred to influence the individual, and

16.4. whether the entity uses third parties in the provision of online marketing materials and if so, the details of those parties and information regarding the appropriate method of opting-out of those materials.

16.5. Repeal APP 7 in light of existing protections in the Act and other proposals for reform.

KPMG response

In relation to direct marketing, KPMG restates the following points from our submission to the Issues Paper:

Our view is that the continuation of the opt-out system in relation to consent for direct marketing is consumer-focussed and effectively allows individuals to choose the extent of their engagement with an APP entity consistent with the current Spam Act requirements. Whilst the use of direct marketing has pivoted to digital and at size and scale, the ability for consumers to simply un-subscribe or withdraw their consent to direct marketing at any point has generally not been inhibited. In practice, we understand APP entities rarely directly market without an understanding that the individual has either consented to be contacted or there is an awareness that their information is being used for this purpose. Due to the nature of brand and reputational damage when APP entities directly market without that consent or reasonable expectation, again, the current system balances the requirements of an APP entity to generate marketing contacts with its conduct within the marketplace.

It is our view that APP 7 has a role to play in relation to regulating the use and disclosure of personal information and provides specific protection for consumers in relation to direct marketing. KPMG would welcome streamlining and clarification of the obligations, particularly having regard to new online forms of direct marketing and targeting which are not clearly covered by current provisions.

The fair and reasonable protection works to safeguard the use of personal information for marketing purpose. While the definition of fair and reasonable could be viewed as quite broad and therefore could lend itself well to safeguarding against the inappropriate use of personal information for direct marketing, it should also be considered that the argument could also go the other way. For example, fair and reasonable could be interpreted to support the use of personal information for marketing. Nonetheless, the right to object should be the primary provision which gives consumers the power to decide how their information is used.

Finally, there is already duplication between the Privacy Act and the Spam Act with respect to direct marketing and we suggest that the Review of the Privacy Act considers any duplication.

FINDING 16: KPMG considers that APP 7 should not be removed unless appropriate protections and rights are introduced including the primary right to object.

17. Automated decision-making

17.1. Require privacy policies to include information on whether personal information will be used in automated decision-making which has a legal, or similarly significant effect on people's rights.

KPMG response

KPMG supports the proposed option in the Discussion Paper which requires privacy policies to include information on whether personal information will be used in automated decision making. Transparency and consent for the use of personal data in this way is important. Furthermore, where personal information will be used in automated decision making, KPMG considers that there should be an option to opt out from data being used in this way with reasonable alternative options to avoid a complete denial of services. Consideration should also be given to algorithms and processes that can reveal and/or leverage undisclosed personal information through a combination of multiple data sources.

FINDING 17: KPMG supports the proposed option 17.1 on automated decision-making. Where personal information will be used in automated decision making, KPMG considers that it should be transparent and there should be an option to opt out from personal information being used in this way.

18. Accessing and correcting personal information

18.1. An organisation must identify the source of personal information that it has collected indirectly, on request by the individual, unless it is impossible or would involve disproportionate effort.

18.2. Introduce the following additional ground on which an APP organisation may refuse a request for access to personal information:

– the information requested relates to external dispute resolution services involving the individual, where giving access would prejudice the dispute resolution process.

18.3. Clarify the existing access request process in APP 12 to the effect that:

– an APP entity may consult with the individual to provide access to the requested information in an alternative manner, such as a general summary or explanation of personal information held, particularly where an access request would require the provision of personal information that is highly technical or voluminous in nature; and

– where personal information is not readily understandable to an ordinary reader, an APP entity must provide an explanation of the personal information by way of a general summary of the information on request by an individual.

KPMG response

KPMG supports the proposals at section 18 and provide the following points for consideration.

In relation to 18.1, it is our view that that the Review may need to consider a potential further update to the *certain matters* notification requirement under APP 5 where collection is indirect. For example, whether an organisation should be required to identify the source of information when providing a notification under APP 5 for indirect collection, rather than on request.

Proposal 18.2 may need to be expanded to *existing or anticipated* external dispute resolution services for greater consistency with the legal proceedings ground on which an APP organisation may refuse a request for access to personal information.

Finally, consideration could also be given to the level of reason applied to the access request process at proposal 18.3. For example, providing an individual print out of the information held may be fairly simple, however providing an explanation or summary may be more time intensive.

19. Security and destruction of personal information

19.1. Amend APP 11.1 to state that 'reasonable steps' includes technical and organisational measures.

19.2. Include a list of factors that indicate what reasonable steps may be required.

19.3. Amend APP 11.2 to require APP entities to take all reasonable steps to destroy the information or ensure that the information is anonymised where the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under the APPs.

KPMG response

KPMG reaffirms the position taken in our submission to the Issues Paper in relation to proposals 19.1. and 19.2:

In our view the requirements placed on entities to destroy or de-identify personal information are appropriate and balanced. The challenge entities face is the potentially conflicting requirements of other laws and regulations to maintain records as well as the timely and effective destruction of digital data given the way it is stored and backed up.

In relation to 19.3, understanding what information to keep and disposing of information that is no longer needed is an important part of effective information management. When processing personal information, KPMG supports the proposal that APP entities should take *all* reasonable steps to destroy or anonymise information where the entity no longer needs the information for any purpose for which the information may be used or disclosed according to the APPs. KPMG considers that the disposal must be done responsibly through a clear understanding of:

- APP entities' business functions;
- The value of the information to the business;
- Legislative retention requirements including information of historical value (e.g. personal information is part of a Commonwealth record); and
- The technology that supports the information.

It would also be beneficial to provide a definition and clear guidance on what constitutes truly anonymised (de-identified) data and what methods are accepted within the Australian environment. Providing clear guidance will allow APP entities to implement the appropriate mechanisms to ensure data is rendered anonymous.

FINDING 18: In KPMG's view the requirements placed on entities to destroy or de-identify personal information are appropriate and balanced.

FINDING 19: When processing personal information, KPMG supports proposal 19.3 that APP entities should take all reasonable steps to destroy or anonymise information where the entity no longer needs the information for any purpose for which the information may be used or disclosed according to the APPs.

20. Organisational accountability

20.1. Introduce further organisational accountability requirements into the Act, targeting measures to where there is the greatest privacy risk:

- Amend APP 6 to expressly require APP entities to determine, at or before using or disclosing personal information for a secondary purpose, each of the secondary purposes for which the information is to be used or disclosed and to record those purposes.

KPMG response

KPMG supports the proposal in the Discussion Paper to introduce further organisational accountability requirements into the Act, including the amendment of APP 6 to expressly require APP entities to determine and record the secondary purposes for which personal information will be used or disclosed, at or before using or disclosing the personal information for a secondary purpose. KPMG considers that this amendment is particularly important in the event of secondary purposes entailing high risk activities such as the use or disclosure of an individual's location data, even if consent is obtained from the individual.

KPMG also suggests the amendment of additional APPs could be considered to further increase organisational accountability under the Act. For instance, consideration may be given to amending APP 3 to expressly mandate that at the time of collection of personal information, entities are required to determine the exact purposes for which an individual's personal information will be collected, used or disclosed and to document those purposes. Likewise, consideration may also be given to amending APP 2 to expressly state the scenarios requiring entities to anonymise or pseudonymise personal information, and/or including explicit requirements for entities to adhere to with respect to third party data transfers under APP 11.

FINDING 20: KPMG supports proposal 20.1 to introduce further organisational accountability requirements into the Act, including the amendment of APP 6 as outlined at 20.1. The amendment of additional APPs could also be considered to further increase organisational accountability under the Act.

21. Overseas data flows

21.1. Amend the Act to introduce a mechanism to prescribe countries and certification schemes under APP 8.2(a).

21.2. Standard Contractual Clauses for transferring personal information overseas be made available to APP entities to facilitate overseas disclosures of personal information.

21.3. Remove the informed consent exception in APP 8.2(b).

21.4. Strengthen the transparency requirements in relation to potential overseas disclosures to include the countries that personal information may be disclosed to, as well as the specific personal information that may be disclosed overseas in entity's up-to-date APP privacy policy required to be kept under APP 1.3.

21.5. Introduce a definition of 'disclosure' that is consistent with the current definition in the APP Guidelines.

21.6. Amend the Act to clarify what circumstances are relevant to determining what 'reasonable steps' are for the purpose of APP 8.1.

KPMG response

In relation to overseas data flows, and specifically APP 8.2, KPMG restates the position from our Issues Paper submission:

The effectiveness of the APP8.2(a) and (b) exceptions do 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 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 APP8.1 assessment.

The requirements for obtaining valid consent for the purposes of relying on APP8.2(b) means its application is potentially very limited save in some very specific cases, otherwise the validity of the consent is uncertain.

We suggest that these APP8.2 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 also supports the adoption of a model similar to the European Union's Standard Contractual Clauses (SCC) model that's 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.

FINDING 21: KPMG considers that an equivalency mechanism similar to the adequacy mechanism under GDPR would provide certainty and reduce burdens on business, without introducing any impact on individuals.

22. Cross Border Privacy Rules and domestic certification

22.1. Continue to progress implementation of the CBPR system.

22.2. Introduce a voluntary domestic privacy certification scheme that is based on, and works alongside CBPR.

KPMG response

KPMG restates the position on cross border privacy rules (CBPR) from our submission to the Issues Paper:

The APEC Cross-Border Privacy Rules (CBPR) has not yet been introduced. This system is a government-backed data privacy certification that companies can join to demonstrate compliance with internationally recognised data privacy protections. The CBPR System implements the PEC Privacy Framework endorsed by APEC Leaders in 2005 and updated in 2015. Any further take-up or endorsement of the CBPR should be carefully considered in the context of the overall objective and net benefits.

FINDING 22: Any further take-up or endorsement of the CBPR should be carefully considered in the context of the overall objective and net benefits as well as the frameworks established by the reformed Act.

Part 3: Regulation and enforcement

23. Enforcement

23.1. Create tiers of civil penalty provisions to give the OAIC more options so they can better target regulatory responses including:

– A new mid-tier civil penalty provision for any interference with privacy, with a lesser maximum penalty than for a serious and repeated interference with privacy.

– A series of new low-level and clearly defined breaches of certain APPs with an attached infringement notice regime.

23.2. Clarify what is a 'serious' or 'repeated' interference with privacy.

23.3. The powers in Part 3 of the Regulatory Powers (Standard Provisions) Act 2014 (Regulatory Powers Act) would apply to investigations of civil penalty provisions in addition to the IC's current investigation powers.

23.4. Amend the Act to provide the IC the power to undertake public inquiries and reviews into specified matters.

23.5. Amend paragraph 52(1)(b)(ii) and 52(1A)(c) to require an APP entity to identify, mitigate and redress actual or reasonably foreseeable loss. The current provision could be amended to insert the underlined:

– a declaration that the respondent must perform any reasonable act or course of conduct to identify, mitigate and redress any actual or reasonably foreseeable loss or damage suffered by the complainant/those individuals.

23.6. Give the Federal Court the power to make any order it sees fit after a section 13G civil penalty provision has been established.

23.7. Introduce an industry funding model similar to ASIC's incorporating two different levies:

– A cost recovery levy to help fund the OAIC's provision of guidance, advice and assessments, and

– A statutory levy to fund the OAIC's investigation and prosecution of entities which operate in a high privacy risk environment.

23.8. Amend the annual reporting requirements in the AIC Act to increase transparency about the outcome of all complaints lodged including numbers dismissed under each ground.

23.9. Alternative regulatory models

- **Option 1** – Encourage greater recognition and use of EDRs. APP entities that handle personal information could be required to participate in an EDR scheme. APP entities that are not part of a recognised EDR scheme could be required to pay a fee for service to the OAIC as the default complaint handling provider if a complaint is made against them.
- **Option 2** – Create a Federal Privacy Ombudsman that would have responsibility for conciliating privacy complaints in conjunction with relevant EDR schemes.
- **Option 3** – Establish a Deputy Information Commissioner – Enforcement within the OAIC.

KPMG response

KPMG's position remains consistent with our submission to the Issues Paper regarding enforcement powers under the Act and the role of the OAIC. Entities currently must manage and comply with a range of regulatory requirements that exist in overlapping and in some cases fragmented data-related frameworks at both a State and Federal level. The Review provides an opportunity to carefully consider how the Act interacts with these frameworks.

In addition to the points raised in the previous submission, we note the following points which expand on our view.

When considering enforcement options, KPMG recommends consideration of which regulatory model will have the capacity, resources and appetite to best enforce regulation or issue penalties. This has been a challenge in Europe where the relevant authority has been criticised for a lack of enforcement.

The Review could consider a range of tools, such as a combination of an industry-funded model (similar to the Australian Securities and Investments Commission), introduction of tiers of civil penalty provisions to give the OAIC more options to better target regulatory responses and proposed Options 1 and/or 2 may be suitable. A Federal Privacy Ombudsman and the use of external dispute resolution (EDR) schemes similar to the Australian Financial Complaints Authority (AFCA) may be worth considering.

As mentioned in our Issues Paper submission, there is a risk of additional regulatory burden on entities that must respond to multiple regulators on essentially similar privacy matters, as well as confusion for consumers. The establishment of a centralised Federal Privacy Ombudsman to support and strengthen privacy enforcement may alleviate this.

FINDING 23: In KPMG's view there is a potential risk of additional burden on entities that must respond to multiple regulators on essentially similar matters, as well as confusion for consumers, and this overlap should be carefully considered as part of the Review. The establishment of a centralised Federal Privacy Ombudsman (Option 2) to support and strengthen privacy enforcement may alleviate this.

FINDING 24: When considering enforcement options, KPMG recommends consideration of which regulatory model will have the capacity, resources and appetite to best enforce regulation or issue penalties.

24. A direct right of action

24.1. 25.1 Create a direct right of action with the following design elements:

- The action would be available to any individual or group of individuals whose privacy has been interfered with by an APP entity.
- The action would be heard by the Federal Court or the Federal Circuit Court.
- The claimant would first need to make a complaint to the OAIC (or FPO) and have their complaint assessed for conciliation either by the OAIC or a recognised EDR scheme such as a relevant industry ombudsman.
- The complainant could then elect to initiate action in court where the matter is deemed unsuitable for conciliation, conciliation has failed, or the complainant chooses not to pursue conciliation. The complainant would need to seek leave of the court to make the application.
- The OAIC would have the ability to appear as amicus curiae to provide expert evidence at the request of the court. Remedies available under this right would be any order the court sees fit, including any amount of damages.

KPMG response

KPMG recommends that careful consideration should be given to inserting a direct right of action in the Act. In our view it would not be the most appropriate mechanism to include in the context of how the regulatory framework operates. The provision in section 13G of the Act and the powers and functions of the Information Commissioner enable the impacts of serious privacy breaches to be addressed. The remedies in the Act as well as other legislation and the common law in our view provide the appropriate balance.

Should a direct right of action be created, KPMG suggests the following points be considered:

- Including stipulated time constraints in relation to lodging a complaint with OAIC and thereafter with the Federal Court or the Federal Circuit Court;
- Provide greater clarity on the circumstances and scenarios an individual can make a complaint to the Federal Court or the Federal Circuit Court; and
- Thresholds should be considered for a complainant to lodge the application with the Federal Court or the Federal Circuit Court.

FINDING 25: KPMG submits that careful consideration should be given to inserting a direct right of action in the Act. In our view it would not be the most appropriate mechanism to include in the context of how the regulatory framework operates.

25. A statutory tort of privacy

25.1. Option 1: Introduce a statutory tort for invasion of privacy as recommended by the ALRC Report 123.

25.2. Option 2: Introduce a minimalist statutory tort that recognises the existence of the cause of action but leaves the scope and application of the tort to be developed by the courts.

25.3. Option 3: Do not introduce a statutory tort and allow the common law to develop as required. However, extend the application of the Act to individuals in a non-business capacity for collection, use or disclosure of personal information which would be highly offensive to an objective reasonable person.

25.4. Option 4: In light of the development of the equitable duty of confidence in Australia, states could consider legislating that damages for emotional distress are available in equitable breach of confidence.

KPMG response

As per KPMG's submission to the Issues Paper, in our view, a tort of privacy would not be the most appropriate mechanism to include in the context of how the regulatory framework operates. The provision in section 13G of the Act and the powers and functions of the Information Commissioner enable impacts of serious privacy breaches to be addressed and remedied appropriately in the Act, other legislation and the common law.

KPMG considers that Option 3 outlined at point 26.3 is most aligned with this view. This option proposes to not introduce a statutory tort and allow the common law to develop as required. However, we do not support extending the application of the Act to individuals in any non-business capacity, which would have a significant impact.

KPMG believes that a statute may fail to capture activities that were not considered when enacting the statute and may also become outdated quickly either due to technological developments or regulatory change.

Additionally, through the precedent set by Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd in 2001, the High Court has left open the possibility for the development of the common law tort for a breach of privacy.

There are a number of points for consideration if Option 3 is adopted, including the uncertainty surrounding whether individuals can seek damages for emotional distress in an action for breach of confidence in Australia, and that an action for breach of confidence may be less effective following a wrong disclosure compared to being taken pre-emptively to prevent a disclosure.

Finding 26: KPMG considers that a statutory tort of privacy would not be the most appropriate mechanism to introduce in the Act in any form, whether in relation to private sector entities or individuals in a non-business capacity.

26. Notifiable Data Breaches scheme

26.1. 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.

KPMG response

KPMG re-states the following position from our Issues Paper submission regarding the impact of the Notifiable Data Breach (NBD) Scheme.

In our view, entities' practices have changed since the commencement of the NDB Scheme, largely in the detection and response aspects of breach management. We have observed that enhancements to the prevention of breaches appears to be more focussed on education and awareness. We consider that the NDB Scheme has gone some way in lifting privacy awareness and helping to advocate the need to take privacy, data security and training seriously.

However, there has been less focus on improvement of technical controls to support breach prevention and protection as a direct consequence of the NDB Scheme which is an area we consider entities should be encouraged to also focus on.

An area where clarity would be welcome was demonstrated by the data breach of an online recruitment services organisation PageUp which impacted multiple Australian entities and resulted in confusion about which entity should be notifying, individuals were burdened with multiple breach notices and the privacy benefits of this were unclear.

In addition, we refer to KPMG's submission to the Department of Home Affairs on strengthening Australia's cyber security regulations and incentives , which discusses the potential for a cyber security code to be introduced in the Act. The development of a risk-based legislated code that outlines clear technical and operational requirements for all regulated organisations, large and small, would be beneficial to provide a clearer data security framework. The development of such a code or set of standards would provide a baseline which entities could follow to support their resilience.

27. Interactions with other schemes

27.1. The Attorney General's Department develop a privacy law design guide to support Commonwealth agencies when developing new schemes with privacy-related obligations.

27.2. Encourage regulators to continue to foster regulatory cooperation in enforcing matters involving mishandling of personal information.

27.3. Establish a Commonwealth, state and territory working group to harmonise privacy laws, focusing on key issues.

KPMG response

KPMG re-states the position from our Issues Paper submission regarding interactions between the Act and other regulatory schemes. KPMG also notes that the OP legislation and the Critical Infrastructure Bill are further examples of regulation that overlap the Act and can create further confusion and regulatory burden.

Separate privacy protections for addressing specific privacy risks and concerns

KPMG recognises that some specific privacy risks and concerns may require specific protections. However, rather than the creation of additional, separate regulatory regimes, we suggest that it would be preferable to address such situations under the framework of the Act, including through the code-making powers in Part IIIB of the Act.

This would assist in ensuring that any additional obligations or protections were consistent with the broader Act obligations and protections, reducing the risks of uncertainty and complexity for both regulated entities and individuals. This has been effectively done in relation to the COVIDSafe app framework.

The collection and use of biometric data through the global acceleration in the development and use of 'biometric technologies', in particular facial recognition technology (FRT) (comprising software, AI and other surveillance mechanisms) is a specific area that requires further consideration, given the privacy risks and impacts. The Australian Human Rights Commission released a discussion paper on the interaction between human rights and emerging technologies which includes consideration of the privacy related issues. 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.

Harmonisation of privacy protections under Commonwealth law – addressing fragmentation

Broadly, KPMG agrees that some (not necessarily all) of the Commonwealth laws offering privacy protections address particular issues that may be appropriately addressed in legislation other than the Privacy Act.

In some instances, however, the existence of multiple privacy regulatory schemes can create uncertainty or duplication. For example, elements of the direct marketing requirements in both APP 7 and the Spam Act 2003 (Cth) may be seen as unnecessary given that the requirements of both schemes are broadly similar (e.g. the requirement of a functional opt-out mechanism). Another example is the overlapping data breach notification regimes.

Other matters

Small business exemption and employee records exemption

KPMG notes that a number of questions were raised in relation to the small business and employee record exemptions, although no options for reform were outlined. KPMG supports the further exploration of the matters raised in the Discussion Paper and refer to our submission to the Issues Paper, in particular noting the following:

Any changes to the small business and employee records exemptions will have the most significant impact in terms of expanding the privacy regulatory framework in the private sector to more organisations and imposing additional regulation. Removing these exemptions will help bring the Act into alignment with the GDPR. The purpose of their removal and 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.

Key authors and contacts

Kate Marshall
Head of KPMG Law

Kelly Henney
Compliance & Conduct Leader, Privacy & Data Protection

Mark Tims
Head of Technology Risk & Cyber Security

Veronica Scott
Privacy, Digital & Data Protection Lead, KPMG Law

Ali Akbari
Artificial Intelligence Capability Lead Innovation, Solutions & Ventures

Matthew Quick
Director, Technology Risk & Cyber

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

Angela Dally
Associate Director, Privacy

Kath Slack
Associate Director, Privacy

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

Danica Ferrone
Associate Director, Compliance & Conduct, Privacy & Data Protection

Joe Green
Manager, Management Consulting

Mark Dunning
Manager, Compliance & Conduct, Privacy & Data Protection

Rob Griffiths
Manager, Deals Tax & Legal

Steph Cosentino
Senior Consultant, Deals Tax & Legal

Jason Kaye
Senior Consultant, Deals Tax & Legal

Leah Roy
Senior Consultant, Compliance & Conduct, Privacy & Data Protection

Aaron Wunsh
Senior Consultant, Compliance & Conduct, Privacy & Data Protection

Joanne Ewen
Senior Consultant, Privacy

Sophie Finemore
Associate Director, Regulatory Affairs

Olivia Spurio
Senior Consultant, Government & Regulatory Affairs

Sam Lynch
Senior Manager, Government & Regulatory Affairs

KPMG.com.au

824105066DTL