27 November 2020

**Attorney-General's Department**

Submitted Electronically

# BSA COMMENTS ON THE REVIEW OF THE AUSTRALIAN *PRIVACY ACT 1988*

BSA | The Software Alliance (**BSA**) appreciates the opportunity to provide comments to the Australian Government on the Review of the Privacy Act 1988 and the associated Australian Privacy Principles (**APP**). [1] BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA's members[2] are among the world's most innovative companies, creating software solutions that spark the economy. BSA member companies have made significant investments in Australia and we are proud that many Australian organisations and consumers continue to rely on our members' products and services to support Australia's economy.

BSA members are enterprise solutions providers that create the software-enabled products and services that power other businesses. They offer tools including cloud storage services, customer relationship management software, human resources management programs, identity management services, cybersecurity solutions, and collaboration software. These enterprise software companies are in the business of providing privacy protective solutions and their business models do not depend on monetizing users' data. BSA members recognize that companies must earn consumers' trust and act responsibly with their personal data.

As such, BSA advocates globally for the implementation of national personal data protection laws that increase the transparency of personal data collection and use; enable and respect informed choices by providing governance over that collection and use; provide consumers with control over their personal data; provide robust security; and promote the use of data for legitimate business purposes.[3] BSA also advocates for the international interoperability of national personal data protection regimes. This is an essential component of the digital economy and should enable and encourage international transfers of personal data. Where differences exist among varying privacy regimes, BSA encourages governments to create tools to bridge those gaps in ways that both protect privacy and facilitate the free flow of data.[4]

---

[1] Review of the Privacy Act 1988, https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988

[2] BSA's members include: Adobe, Amazon Web Services, Atlassian, Autodesk, AVEVA, Bentley Systems, Box, Cadence, Cisco, CNC/Mastercam, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Sitecore, Slack, Splunk, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

[3] See BSA's Global Privacy Best Practices at: https://www.bsa.org/files/policy-filings/A4_2018_BSA_Global_Privacy_Best_Practices.pdf

[4] BSA Privacy Framework, https://www.bsa.org/policy-filings/bsa-privacy-framework

300 Beach Road
#25-08 The Concourse
Singapore 199555

P: +65 6292 2072
F: +65 6292 6369
W: bsa.org

Regional Representative Office
UEN: S97RF0005K

BSA strongly supports the Australian Government's commitment to improve the personal data protection regime that strengthens accountability and consumer trust in personal data management while enhancing flexibility for the responsible use of personal information to drive innovation and economic growth and recovery. BSA welcomes the review of the *Privacy Act 1988* (the **Act**) and provides comments below based on the associated *Privacy Act Review Issues Paper* (the **Paper**).[5]

In our comments below, we provide the following main recommendations:

- Establish a clear distinction between the roles and responsibilities of personal data controllers and personal data processors.
- Keep the Act's the current definition of personal information and exclude technical information that is not reasonably linkable to a specific individual, or has been de-identified by robust technical or organisation methods.
- Recognise several equally valid grounds for lawful data processing of personal information and provide a new ground for the lawful processing of personal information on the basis of legitimate interests.
- Do not introduce an individual right of action.
- Individuals should have a right to request a data controller to erase their personal data from the controller's systems, with consideration for factors such as compliance with legal obligations and technical feasibility.
- The Act should enable and encourage global data flows by allowing for multiple inter-operable mechanisms for the transfer of personal information while ensuring the privacy and security of personal information.

## Objectives of the Act

The Paper invites feedback on the "objects" outlined in section 2A of the Act.[6] These include promoting the protection of the privacy of individuals, recognizing that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities, promoting responsible and transparent handling of personal information by entities, providing a basis for nationally consistent privacy regulation and practices, facilitating free flow of information across national borders, providing a means of redress, and implementing Australia's international obligations in relation to privacy.

These objectives are foundational to any privacy law and remain appropriate for the Australian privacy regime.

As noted in the Paper, the precursor report to the Review by the Australian Competition and Consumer Commission[7] recommended considering whether it remains appropriate for the objectives to require the protection of privacy to be balanced with the interests of business in carrying out their functions or activities.

The protection of privacy and the ability for businesses to use data are not mutually exclusive goals. Both objectives underpin a data protection framework that protects the privacy rights of individuals, supports consumer trust in the digital economy, and enables innovation in data-intensive solutions that drives economic growth and recovery. Such policies enable the application of advanced technologies, such as cloud computing, data analytics, and artificial intelligence to solve some of

[5] Privacy Act Review Issues Paper, https://www.ag.gov.au/system/files/2020-10/privacy-act-review--issues-paper-october-2020.pdf

[6] Ibid., p15

[7] Australian Competition and Consumer Commission, Digital Platforms Inquiry, https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf, p439, 477

societies' most significant challenges, from tackling climate change to responding to public health emergencies and many others.

## Controller/Processor separation

The Act currently regulates APP entities, defined as agencies or organisations subject to the APP[8] and imposes on these entities a common set of obligations. In doing so, the Act fails to recognize a critical distinction that is foundational to privacy laws worldwide, which distinguish between businesses that decide how and why to collect an individual's data (and thus act as data "controllers") and businesses that process the data on behalf of another company (acting as "processors" of the data).

The approach of regulating APP entities reflects the Act's origins, first as a regulation that applied only to public-sector entities and then expanded by the *Privacy Amendment (Private Sector) Act 2000* to reach private-sector entities. Since that time, however, it has become clear that the distinction between data controllers and data processors, regardless of whether these or other terms are used, is foundational to privacy laws worldwide — and is needed to ensure that such laws create role-based obligations that protect consumer privacy and create clear obligations for the different businesses involved in handling consumers' data.[9] To better achieve the objectives of the Act, we urge you to recognize the unique roles of data processors and data controllers as you revise the Act. This will ensure the obligations placed on businesses are in accordance to their different roles in handling the consumer data, reflect technical realities, and provide clearer mechanisms for individuals to assert their rights.

By distinguishing between data controllers and data processors, a privacy law can clearly tailor obligations to different types of companies based on those companies' roles in collecting and using an individual's personal information. That is vital in today's digital economy, where an individual may purchase a service from one consumer-facing company, but that company may rely on enterprise service providers to store, analyze, and process the data in connection with that service. Each company that processes an individual's personal information should be subject to strong obligations to safeguard that information — but those obligations should vary according to the different roles these companies play. Indeed, in many cases, failing to distinguish between these different types of companies can inadvertently undermine consumer privacy.

For example, if both controllers and processers are required to obtain consumers' consent to process their data, it would not only inundate consumers with duplicative consent requests from multiple companies for the same processing activity (rendering each request less meaningful), but it would also create security risks (by requiring consumers to grant or deny permissions to data processors they do not know) and new privacy risks (by potentially requiring data processors to have knowledge of data they otherwise would not access).

The Paper highlights an example where this distinction would help to clarify the obligations imposed by the Act.[10] In discussing APP 8, the Paper considers an example of an entity engaging an overseas contractor to perform services on its behalf. Depending on the nature of those services, the movement of personal information could either be deemed as a "disclosure" for which APP 8 applies, or a "use" for which APP 8 is not applicable. The Paper notes that the provision of data to a cloud service provider for the limited purpose of storing the information would be a "use" rather than a "disclosure." However, the distinction between "use" and "disclosure" is not clear, and it would be better to evaluate

---

[8] As defined in *Privacy Act 1988, Australian Privacy Principles guidelines — Chapter B: Key Concepts,* *https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-b-key-concepts/#:~:text=2%20An%20%27APP%20entity%27%20is,(s%206(1)).&text=3%20An%20%27organisation%27%20is%20defined,a%20partnership*

[9] The controller/processor distinction is crucial to a host of privacy laws including the EU General Data Protection Regulation and the California Consumer Privacy Act. In addition, leading international privacy standards, including ISO 27701, and voluntary frameworks that ensure data can be transferred across national borders, such as the APEC Cross Border Privacy Rules, also distinguish between controllers and processors. Other laws, such as those in Japan, Singapore, and Malaysia, recognize this distinction while using different terms. BSA published a paper highlighting the importance of this distinction. See BSA, The Global Standard: Distinguishing Between Controllers and Processors in Privacy Legislation, https://www.bsa.org/files/policy-filings/03032020controllerprocessor.pdf

[10] Privacy Act Review Issues Paper, https://www.ag.gov.au/system/files/2020-10/privacy-act-review--issues-paper-october-2020.pdf, p56.

the transfer based on which company "controls" the data and which is simply following the instructions of its enterprise customer to "process" the datait.

By distinguishing between data controllers and data processors (rather than "uses" and "disclosures"), the guidance could clearly set out what obligations apply to data controllers, such as obtaining consent — and those that apply to third parties that process the data on the data controllers' behalf and at their direction, such as appropriately securing the data.

Because the Act does not clearly distinguish between these two different roles, companies are often left to assign obligations between themselves by contract, which can vary significantly across industries and companies. Updating the Act to clearly define controllers and processors — and to assign each obligations that are appropriate to their respective roles — would provide greater clarity for consumers and businesses. It would also ensure that policymakers can better achieve the objectives of the Act. Several examples below illustrate how distinguishing between controllers and processors will improve the functioning of the Act.

### *Example 1 — HR data outsourcing*

The concerns raised by a lack of controller/processor distinction are compounded by other aspects of the Act, including its treatment of employee information, which can be a significant source of confusion for businesses subject to the Act. In particular, even when a company holds data about its own employees that may be exempt from the Act, the same data may nonetheless be covered by the Act if that company transfers it to a processor to store or otherwise process the data.

For example, Company ABC may want to use an outsourced HR cloud data service provider DEF. When ABC holds data about its employees, that data is not subject to the Act. However, when the same data is transferred to DEF, it may be covered by the Act since the relevant employees are not employed by DEF. This result is not consistent with the aim of exempting employee information — since the exemption should turn on the type of data (e.g., employee data) rather than the company holding the data. It also results in the same set of data being simultaneously not subject to the Act (from the perspective of ABC) and subject to the Act (from the perspective of DEF).

### *Example 2 — Consumer rights requests*

When a privacy law does not distinguish between controllers and processors, individuals may be unsure about which company they should approach to exercise their individual rights. This can frustrate consumers, who may end up being forced to reach out not only to the consumer-facing companies they interact with, but also the data processors that store and process data on behalf of those consumer-facing businesses.

This can not only be inefficient and confusing for consumers, but also creates new risks to their privacy. Responding to consumer rights requests — such as requests to access, correct, or delete personal data — requires knowing what is in that data. Controllers interact with consumers and decide when and why to collect their data. For that reason, many privacy laws, including the EU's General Data Protection Regulation (**GDPR**), require data controllers to respond to consumer rights requests. Moreover, data controllers must decide if there is a reason to deny a consumer's request, such as when a consumer asks to delete information subject to a legal hold or asks to correct information that is already accurate. Data controllers are also in the best position to confirm that the consumer requesting access or changes to the data is the authorized data subject.

Data processors, in contrast, often do not know the content of the data they process and may be contractually prohibited from accessing or reviewing the data to protect the privacy of that information. It is not appropriate for processors to respond directly to a consumer's request. Doing so creates both security risks (by providing data to consumers they do not know) and privacy risks (by reviewing data they otherwise would not be authorized to access). Instead, privacy laws should clearly distinguish between data controllers and data processors, assign controllers the responsibility of responding to consumer rights requests, and require processors to provide controllers with tools the data controller can use to collect data needed to respond to a consumer's request when that data is held by the data processor.

### *Example 3 — Data breach notification*

Failing to distinguish between data controllers and data processors can also lead to unintentional results in responding to data breaches.

To be clear, both data controllers and data processors should be required to safeguard the data that they hold, and should develop, implement, and maintain administrative, technical, and physical safeguards that are reasonably designed to protect the security and confidentiality of personal data. At the same time, if a potentially notifiable breach has occurred, the Act requires companies to assess whether the breach is notifiable.

A data processor is not likely to have access to the information needed to make this assessment, since, as a way to safeguard the privacy of personal data it is processing on behalf of the data controller, the data processor may be contractually prohibited from reviewing or analyzing such data . By distinguishing between data controllers and data processors, a privacy law can ensure that data controllers have the obligation to make this assessment, but that both data controllers and data processors should implement strong data security safeguards.

## Definition of "personal information"

The Paper discusses the current definition of personal information under the Act and seeks feedback on issues regarding its scope with regard to technical information, inferred personal information, and de-identified, anonymized, and pseudonymized information.[11]

BSA recommends that the scope of information included within the definition of personal information should be information that relates to an identified or identifiable consumer. An identifiable consumer is itself defined as one who can be identified, directly or indirectly, through reasonable effort by an entity with the information to which it has access, by reference to an identifier such as a consumer's name, an identification number, location data, an online identifier, or one or more factors specific to the consumer's physical, physiological, or genetic identity. This approach does not focus exclusively on the source of the information, but rather on the relationship between the data and the data subject. The current definition of "personal information" in the Act (i.e. including information or an opinion about an "identified" individual, or an individual who is "reasonably identifiable") is sufficiently broad and likely interoperable with definitions found in other personal information protection laws.

To the extent the current definition of personal information subject to the Act is revised, any revisions should focus on personal information that, if mishandled, would have a meaningful impact on a consumer's privacy. If the scope of the definition is not limited in this way and the Act's obligations apply to a broad range of data regardless of its context and the risk of harm to specific individuals, the law is likely to have a chilling effect on data-driven innovation, negatively impacting economic growth without a corresponding benefit to personal privacy.

The Paper notes the current lack of clarity regarding technical data and asks whether technical information not reasonably linkable to a specific individual should be explicity included in the definition of personal information.[12] BSA recommends the Privacy Act should continue to exclude from its scope data that is not reasonably linkable to a specific individual, taking into account whether the APP entities collecting or processing such information are reasonably likely to have and use the means available to them to be able to identify such individuals from such information. Just as APPs 3 and 4 distinguish between "solicited" and "unsolicited" personal information, the Act should draw a distinction between different types of technical data based on the concepts of "directly provided personal information" and "inferred personal information".

BSA recommends that the Act exclude from its scope data that is de-identified through robust technical and organizational measures designed to reasonably reduce the risk of re-identification. This creates an incentive for businesses to develop and use strong de-identification techniques which can help reduce privacy and security risks. At the same time, the ability to use de-identified or anonymized data outside the framework of a data protection law can encourage innovative uses of that data, and

[11] Ibid., p19

[12] Ibid., p18

encourage companies to use this de-identified or anonymized data rather than personal data, thus increasing privacy protections.

Finally, we note that to the extent the Act covers pseudonymized data, it should subject that data to less stringent requirements than applied to personal data. Pseudonymous data is generally organized according to a randomly generated identifier that is not used in other datasets, thus mitigating risks that third parties will link the information to a specific individual. Accordingly, privacy laws may encourage companies to use this privacy-protective technique by recognizing pseudonymous data are subject to more flexible requirements than those imposed on personal data which are more readily associated with a specific individual.

## Consent to collect, use, and disclose personal information

Under APP 3, APP entities are permitted to collect personal information without consent if that information is reasonably necessary for one or more of their legitimate functions or activities. APP entities must, however, obtain consent from an individual for the collection of sensitive personal information. Further, under APP 6, APP entities will also need to obtain consent from individuals before using or disclosing personal information unless it is for the primary purpose for which it was collected, or if the individual reasonably expects that their personal information will be used for a secondary purpose, or another prescribed exception applies. Consent under the Privacy Act can be 'express or implied'.

Consent is an important legal basis for the collection, use, and disclosure of personal information, but it should not be the only basis. Providing several independent grounds for lawful data processing is a key feature of a robust personal data protection framework and other grounds for processing should be equally valid. Data protection frameworks should recognize and enable data processing for a range of valid reasons, including legitimate business purposes that are consistent with the context of the transaction or expectations of consumers. Other valid purposes include processing in connection with the performance of a contract; in the public interest or the vital interest of the consumer; and necessary for compliance with a legal obligation. According to the APPs, there are several limited exceptions to consent, referred to as permitted general situations. However, they are recognised as exceptions and not alternate grounds for collection and use in their own right and are currently too narrowly defined.

BSA accordingly recommends that the Australian Government consider adding a new ground for the lawful processing of personal information on the basis of "legitimate interests" of the APP entity. The legitimate interest ground for processing is a well-established feature of data protection frameworks that aims to facilitate the use of personal data for innovative purposes where it may not be suitable or appropriate for the data controller to obtain consent to legitimize data collection, while also ensuring that any risks to the individual rights of data subjects are appropriately taken into account.

Legitimate interests include processing for purposes of fraud detection and prevention; monitoring, detecting, and protecting a network via cybersecurity measures; and updating products and services to ensure they are as accurate and reliable as possible. As enumerating the range of these legitimate interests in statutory language is impractical, including a ground such as "reasonable purpose" or "legitimate interest" would provide companies the flexibility and regulatory certainty to process personal information for these legitimate purposes.

Moreover, by recognising additional grounds for processing beyond consent, privacy laws can reduce the burden on consumers to consent to each expected use of their personal information. Consent is then reserved for situations in which it is most meaningful to consumers — when a use may involve sensitive personal information, or may be unexpected in a given context.

In cases when consent is required, the requirements for obtaining it should be contextual. In settings where consent is appropriate, consent should be provided at a time and in a manner that is relevant to the context of the transaction or the organization's relationship with the consumer. Therefore, it is important the Act continues to recognize the validity of both implied and express consent. In many situations, strengthening consent requirements by requiring express consent may lead to consent fatigue or discourage individuals from using digital products and services.

For example, if an individual using public transportation must provide express consent to allow an electronic gate to collect data every time they swipe a public transportation card, it may create disincentives to using the card or the public transport system.

Similarly, separate consent should only be sought where purposes are unrelated and therefore would not be reasonably expected by an individual. Where consent is appropriate, data controllers should obtain consent and data processors must act on behalf of the data controllers and in line with the data controller's instructions. In the case where purposes have dependencies or are related to each other and where they are reasonably expected, individuals should be allowed to consent to those multiple purposes together.

Any revisions to the Act should consider these contexts and allow flexibility in determining the timing, standard, and mechanism for obtaining consent.

## Individual right of action

BSA recommends that an individual right of action is not introduced to the Act.

Effective enforcement of a privacy law is critical to protecting consumers' privacy, ensuring that organizations meet their commitments and legal obligations, and deterring potential violations. A privacy law can create strong and effective enforcement without including a private right of action.

Consumers and companies need clarity in understanding how the rights and obligations created by any new privacy law will be applied. An agency like the Office of the Australian Information Commissioner (**OAIC**) is well-positioned to provide that clarity, because agencies can create a consistent body of enforcement efforts that demonstrate how the agency will apply the new rights and obligations in a variety of contexts, particularly when combined with informal or formal guidance interpreting the privacy law.

In contrast, enforcement structures that rely on private litigation may only provide that clarity after litigants spend significant amounts of time bringing their cases before courts. Even then, differing decisions by different courts may result in a less certain enforcement environment than a cohesive agency-led approach, and provide less useful guidance to companies that want to understand their obligations in advance.

## Individual's right of erasure

The Issues Paper notes a recommendation by the Australian Law Reform Commission to include a "right of erasure" in the Act.[13] Under this right, APP entities would be required to erase personal information of a consumer upon request without undue delay unless the retention of the information is necessary for the performance of a contract with the consumer, is required under law, or is for an overriding public interest.

We support including mechanisms in privacy laws by which consumers may control their personal data including the right to have their data deleted.

If the Australian Government decides to introduce or define an explicit "right of erasure", it is important to ensure that the obligation to comply with such a request falls upon the APP entity in control of the personal information (acting as a "data controller") and not to the downstream participants of such information (the "data processors"). It should also be clear in the Act that data controllers may deny such requests where the burden or expense of doing so would be unreasonable or disproportionate to the risks to the consumer's privacy; to comply with legal requirements; to ensure network security; to otherwise protect confidential commercial information; for research purposes; or to avoid violating the privacy, free speech, or rights of other consumers.

## Data breach notification

BSA supports reasonable and appropriate personal data breach notification requirements that are consistent with global best practices to provide incentives to ensure robust protection of personal information. Data controllers should notify consumers as soon as practicable after discovering a personal data breach involving the unauthorized access to or loss of unencrypted or unredacted personal data that creates a material risk of identity theft or financial fraud. These actions enable individuals to take protective actions to protect themselves from serious harm.

---

[13] Ibid., p52

To achieve these goals, it is critically important to set the correct threshold for reporting breaches based on risk of harm to individuals, to allow sufficient time for data controllers to report, and to provide appropriate exceptions to the notification requirement.

BSA applauds the Australian Government on the successful implementation of the Notifiable Data Breach (**NDB**) scheme in February 2018 which has led to greater transparency and accountability of entities concerning data breaches in Australia.[14] The NDB has been carefully drafted to avoid requiring APP entities to issue immaterial notices by scoping a NDB to when APP entities have "reasonable grounds" to believe that an "eligible data breach" that will result in "serious harm" to individuals has occurred.

The Paper raises important issues surrounding multi-party breaches and compliance across multiple international frameworks.[15]

Considering multi party breaches, BSA broadly supports the approach recommended by the OAIC whereby entities with the most direct relationships with individuals affected by the data breach carry out the notification. However, the Act could more clearly set out the obligations surrounding a multi-party breach if it distinguishes between data controllers and data processors, as discussed above. In many cases, a data controller may have a direct relationship with a consumer but may entrust data processors to store or process data on their behalf. Those processors interact with the controller, but often do not know the individuals to whom the personal information relates, as they merely hold or process that information on behalf of the data controller and pursuant to the data controller's directions.

Distinguishing between data controllers and data processors can help the Act to properly allocate responsibility for data breach notification. If a data processor suffers a data breach, it should be bound by contract to notify the data controller, who, in turn, should notify data subjects, as soon as practicable, of a personal data breach involving the unauthorized acquisition of unencrypted or unredacted personal data that creates a material risk of identity theft or financial fraud. If the Act is not revised to define data controllers and data processors and set out the appropriate obligations for each, BSA nonetheless encourages that the OAIC's recommendation that entities with the most direct relationships with affected individuals carry out the notification be expressly included in either the Act or the APPs.

BSA recommends that the NDB retain the current flexibility in reporting timeframes.It is impractical to specify a fixed deadline for providing notification in all scenarios. Breaches may occur in a range of different contexts and may be subtle and carried out by highly sophisticated and well-resourced actors, or they may occur in the systems of third parties. Adopting a one-size-fits-all notice deadline ignores the practical realities that may differ in these different scenarios. To the extent a fixed deadline required companies to notify individuals of a potential breach before all relevant facts have been ascertained, it can create confusion and lead to the need for follow-up notifications.

## Security of personal information

The Paper briefly discusses security obligations under APP 11 and asks whether the security requirements under the Act are reasonable and appropriate to adequately protect the personal information of individuals.[16]

BSA supports the current requirements under APP 11 for companies to take reasonable security measures to protect personal information under their control from misuse, interference, loss, unauthorised access, modification, or disclosure. This broad description recognises that companies are diverse in terms of technologial infrastructure, experience different types of risk, and confront different threats and threat actors. Overly directive regulation focusing on specific methods or controls, or strict compliance to local standards, can have a disruptive impact on companies' attempts to properly secure personal information.

---

[14] Office of the Australian Information Commissioner, *Notifiable Data Breaches Scheme 12-month Insights Report* (Report 13 May 2019)

[15] Privacy Act Review Issues Paper, https://www.ag.gov.au/system/files/2020-10/privacy-act-review--issues-paper-october-2020.pdf, pp79-81

[16] Ibid., p50, p52

Outcome-based approaches that are based on risk management principles allow organisations to prioritise their efforts against the most important risks, take full advantage of technologies such as multi-factor authentication and encryption, and use privacy enhancing strategies such as differential privacy to best secure personal information.

## Overseas data flows and third-party certifications

The seamless transfer of data across international borders is critical to cloud computing, data analytics, and other modern and emerging technologies and services that underpin the global economy. A forward-leaning policy on cross-border data transfers, which is interoperable with international frameworks, is a particularly effective tool to aid policymaker efforts to drive innovation, increase employment, and build economies.

BSA strongly supports the accountability model for overseas data flows, first established by the OECD[17] and subsequently endorsed and integrated in many legal systems and privacy principles, including the Act and APPs. The accountability model provides an approach to cross-border data governance that effectively protects individuals and fosters streamlined, robust data flows by requiring entities that collect personal information to be responsible for its protection, no matter where or by whom it is processed.

The Paper cites the example of how the Act was amended to implement privacy protections for information collected by the COVIDSafe App where specific provisions were introduced to ensure data was stored within Australia and to prohibit the overseas transfer of COVID app data.[18] While governments are rightfully concerned with privacy risks and data security, privacy protection and security are ultimately not dependent on the physical location of the data, or the location of the infrastructure supporting it. They are instead a function of the quality and effectiveness of the mechanisms and controls maintained by the entities controlling or processing the data to protect the data in question. The accountability model therefore continues to be an important tool in increasing privacy and security by requiring entities to ensure that data continues to be properly protected, regardless of where the data is located. The Act's support for the accountability model could be further strengthened by explicitly stating that data localisation is not required under the model.

National data protection and privacy frameworks that are based on a common set of internationally recognized consensus-based principles help global efforts to build interoperable systems and mechanisms that facilitate cross border data transfers. These coordination mechanisms also help to bridge current gaps in international privacy norms while facilitating the safe and secure transfer of personal information. In the context of personal information protection, such mechanisms may include private codes of conduct, contractual arrangements including standard contractual clauses, certifications such as the APEC Cross Border Privacy Rules and Privacy Rules for Processors, seals, or marks, and mutual recognition arrangements, such as adequacy with the GDPR.

The Paper highlights some of these mechanisms and we would encourage the Australian Government to recognize that many of these existing global mechanisms can meet requirements imposed by the Act on international data transfers. Recognizing these mechanisms would align the Act with global best practices and give businesses the flexibility to determine which mechanisms will be better suited for each situation. These mechanisms are incorporated in other data protection frameworks to promote cross-border data flows, including the GDPR, Singapore's Personal Data Protection Act,[19] and Japan's Act on the Protection of Personal Information.[20]

In contrast, if the Australian Government were to create new data transfer mechanisms solely for use by companies transferring data to and from Australia, it may decrease incentives for companies to adopt those measures and would not encourage the widespread use of interoperable mechanisms to facilitate responsible data transfers.

---

[17] The OECD Privacy Framework, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

[18] Privacy Act Review Issues Paper, https://www.ag.gov.au/system/files/2020-10/privacy-act-review--issues-paper-october-2020.pdf, p56

[19] Personal Data Protection Act 2012, https://sso.agc.gov.sg/Act/PDPA2012

[20] Act on the Protection of Personal Information (English), https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf

Similarly, a domestic privacy certification scheme could provide companies a mechanism for demonstrating their compliance with the local privacy laws. However, such a scheme needs to remain voluntary and should be interoperable with other global schemes to help further industry participation and ensure meaningful protections for consumers.

## Conclusion

Effective privacy protections are an essential component of underpinning trust in the digital economy and the protection of personal data is an important priority for BSA members. BSA is grateful for the opportunity to provide these further comments on the proposed amendments to the Act. We remain supportive of the Australian Government's efforts to review and update the personal data protection regime in Australia, responding to the ever-evolving needs of the digital economy and data innovation.

BSA thanks the Australian Government for providing the opportunity to comment on the Review and we look forward to continuing to collaborate with the Government on privacy and personal data protection policies. If you require any clarification or further information in respect of this submission, please contact the undersigned at brianf@bsa.org or +65 8328 0140.

Yours faithfully,

Brian Fletcher

Director, Policy – APAC

BSA | The Software Alliance