21 January 2022

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

**Submitted Electronically to the Attorney-General's Department**

BSA | The Software Alliance (**BSA**)[1] welcomes the opportunity to provide comments to the Attorney-General's Department (**AGD**) on the Privacy Act Discussion Paper (**Discussion Paper**).[2] The Discussion Paper consolidates the substantial stakeholder feedback received on the Privacy Act Review Issues Paper (**Issues Paper**) published in October 2020[3] which was designed to "consider whether the scope of the *Privacy Act 1988* (**the Act**) and its enforcement mechanisms remain fit for purpose."[4]

BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA's members are enterprise solutions providers that create the technology products and services that power other businesses.[5] Our members have made significant investments in Australia, and we are proud that many Australian entities and consumers continue to rely on our members' products and services to support Australia's economy. BSA members recognise that companies must earn their consumers' trust and act responsibly with their personal information. We are encouraged to see that our submission on the Issues Paper[6] was referenced several times in the Discussion Paper.

Many of the proposals in the Discussion Paper, if adopted, would significantly strengthen personal data protections and consumer rights in Australia. Below, BSA encourages the AGD consider nine additional recommendations designed to enhance privacy protections for Australians and improve the international interoperability of Australia's personal data protection rules to facilitate regulatory certainty and cross-border investment in cutting edge services that will drive Australia's post-pandemic economic recovery and job creation. Most importantly, we strongly encourage the AGD to implement a clear distinction between controllers and processors in the Privacy Act, which will

---

[1] BSA's members include: Adobe, Altium, Alteryx, Amazon Web Services, Atlassian, Autodesk, Aveva, Bentley Systems, Box, Cisco, CNC/Mastercam, CrowdStrike, Dassault, DocuSign, Dropbox, IBM, Informatica, Intel, MathWorks, Microsoft, Nikon, Okta, Oracle, PTC, Rockwell, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

[2] Discussion Paper, Review of the Privacy Act 1988, October 2021, https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/user_uploads/privacy-act-review-discussion-paper.pdf.

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

[4] Issues Paper (2020), p. 2.

[5] How Enterprise Software Empowers Businesses in a Data-Driven Economy, January 2021, https://www.bsa.org/files/policy-filings/011921bsaenterprisesoftware101.pdf and appended to this submission.

[6] BSA Comments on the Review of the Australian Privacy Act 1988, November 2020, https://www.bsa.org/files/policy-filings/11272020ausprivacyactrev.pdf (**BSA 2020 Comments**).

300 Beach Road
#30-06 The Concourse
Singapore 199555

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

Regional Representative Office
UEN: S97RF0005K

strengthen protection for consumers and increase interoperability with leading data protection laws worldwide.

## Summary of BSA's Recommendations

- *First*: Implement a clear distinction between the roles and obligations of entities that decide how and why to collect personal information (**controllers**) and those that simply process collected personal information on behalf of another entities (**processors**).

- *Second*: Adjust the definition of personal information such that: (1) information which presents only a remote or hypothetical risk of identifying a specific consumer would *not* be covered by the Act; and (2) location data, should it be listed as an example of personal information, be limited to precise geolocation information relating to an identifiable individual.

- *Third*: Continue to recognise that de-identified information is not subject to the Act, expressly state whether pseudonymised information falls within the definition of personal information, and, to the extent that the Act covers pseudonymised information, subject that information to less stringent requirements than those applied to personal information. The Act should also actively encourage companies to use pseudonymisation.

- *Fourth*: Recognise legitimate interests as a lawful basis for processing personal information and implement guidelines, factors, and checklists to help companies understand how to use this basis.

- *Fifth*: Do *not* amend APP 11.2 to require APP entities to take *all* reasonable steps to destroy or to anonymise personal information that is no longer needed or required. The existing standard in APP 11.2 of taking "such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified" should be retained.

- *Sixth*: Recognise existing mechanisms governing international data transfers, such as the APEC Cross-Border Privacy Rules (**CBPR**) and Privacy Rules for Processors (**PRP**) and, to the extent that new mechanisms governing international data transfers are created, these new mechanisms should remain voluntary and be interoperable with other global schemes. The Act also should retain the informed consent exception in APP 8.2(b).

- *Seventh*: Do *not* introduce an individual right of action or statutory tort for invasion of privacy. If a direct right of action is introduced, the participation of the enforcing agency in the proceedings should be mandatory to enhance regulatory coherence.

- *Eighth*: Retain the employee records exception and ensure that any modifications to that exception recognise the unique aspects of the employer-employee relationship.

- *Ninth*: In respect of individual rights requests, ensure that: (1) any right to object is qualified; (2) any right to erasure is interoperable with emerging international personal data protection frameworks; and (3) the obligation to respond to objections to the collection, use, and disclosure of personal information for the purposes of direct marketing lies with controllers.

## Distinction Between Controllers and Processors

We welcome the Discission Paper's recognition of the importance of distinguishing between controllers and processors.[7] BSA was among the large group of stakeholders that urged the AGD to focus on this issue, because creating a clear distinction between these two different types of entities improves privacy protection for individuals and is foundational to privacy laws in many jurisdictions worldwide.

At present, the Act does not expressly distinguish between controllers and processors; instead, it regulates all Australian Privacy Principles (**APP**) entities[8] and imposes on them a common set of obligations. The Discussion Paper notes that the distinction between controllers and processors is "present in many international data protection regimes" and recognises the benefits of adopting this distinction,[9] but ultimately does not propose to introduce it. **We urge the AGD to introduce the concepts of controllers and processors into the Act in connection with this review**.

BSA also offers views on the three questions posed in the Discussion Paper on the controller/processor distinction:

*Q1: Are there any other advantages or disadvantages of introducing the concepts of data controllers and processors into the Act?*

**There are significant advantages** to introducing the controller and processor concepts into the Privacy Act. Doing so would increase protections for consumers, create more certainty for companies about their obligations under the Act, and align Australia with leading global data protection frameworks.

- *Incorporating the controller/processor distinction would help align Australia with leading global privacy laws*. At the outset, it bears reiterating that the controller/processor distinction is a key feature of privacy laws worldwide.[10] This distinction is necessary in today's digital economy, where an individual may use a service from one consumer-facing entity, but that entity may rely on numerous other enterprise service providers to store, analyse, and process the data in connection with that service. Each entity 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 entities play. Incorporating this distinction and aligning Australia with leading global privacy laws, including the European Union's General Data Protection Regulation (**GDPR**), California's Consumer Privacy Act, Japan's Act on the Protection of Personal Information, and Singapore's Personal Data Protection Act will streamline obligations for Australian entities required to comply with the privacy laws of other jurisdictions and facilitate such entities' participation in the global digital economy.[11]

- *Incorporating the controller/processor distinction improves protection for consumers and provides clarity for business entities.* A clear distinction benefits consumers by helping them understand which entity can best respond to inquiries related to consumers rights or other consumer-facing privacy obligations. As the Discussion Paper recognises, distinguishing between controllers and processors would provide clarity to individuals about the roles of

[7] Discussion Paper (2021), p. 156-158.

[8] Defined as agencies or organisations subject to the APP, per the Australian Privacy Principles Guidelines, Chapter B: Key Concepts, July 2019, https://www.oaic.gov.au/__data/assets/pdf_file/0003/1200/app-guidelines-chapter-b-v1.3.pdf.

[9] Discussion Paper (2021), p. 157.

[10] The Global Standard: Distinguishing between Controllers and Processors in Privacy Legislation, March 2020, https://www.bsa.org/files/policy-filings/03032020controllerprocessor.pdf, and appended to this submission.

[11] Discussion Paper (2021), p. 157.

different entities and help them identify the entity to contact to exercise their rights under the Act. It will also help to ensure that individuals do not receive duplicative consent requests from different entities, where a controller and a processor may both be inadvertently required to seek consent for the same processing activities. Indeed, in many cases, failing to distinguish between these different types of companies can confuse consumers and, more importantly, create data security risks and undermine consumer privacy.

**In terms of potential disadvantages or challenges**, BSA recognises that distinguishing between controllers and processors requires a deep assessment of the Australian privacy framework to identify the obligations in the Act that should be placed on controllers and those that should be placed on processors. Still, we believe the benefits of undertaking that assessment will ultimately outweigh any disadvantages. For example, incorporating this distinction will improve the functioning of the Act in respect of at least three issues considered under the review:

- *Clearer obligations on obtaining consent to collection, use and disclosure of personal information (APPs 3 and 6).* Consent obligations are among the consumer-facing obligations that are appropriately placed on controllers, not processors. A consumer buying a good or service typically interacts with the controller providing that good or service — and may rightly expect the controller to ask their consent to process their personal data for certain purposes. Stating in the Act that this obligation falls on controllers, and not processors, will help to prevent situations in which processors may be required to obtain consent for processing when a controller has already obtained the consumer's consent. Unless consent obligations are clearly placed on controllers, consumers may receive consent requests from multiple companies for the same processing activity, which risks both confusing consumers and leading to "click-fatigue" where individual consumers are inundated with repeated requests that erode the effectiveness of consent obligations.

- *Improved security and clarity when responding to consumer rights requests*. BSA previously expressed support for implementing mechanisms through which consumers may control their personal data, including the right to have their data deleted.[12] We are glad to see that the Discussion Paper proposed introducing a right to request erasure in certain situations. However, processors should not be obliged to respond to such consumer-facing requests, which are best handled by controllers, for several reasons. First, responding to consumer rights requests often requires authenticating the identity of the individual consumer making the request and understanding whether the request should be carried out. Controllers, which generally interact directly with individual consumers and decide when and why to collect personal data, are best positioned to authenticate consumers making requests. Second, controllers are also in a better position to determine if there is a reason to deny an individual consumer's request, including whether an exception to the consumer request is applicable. In contrast, these obligations are ill-suited to processors, which often do not know the consumers making requests, and may be limited in accessing the information stored on their service either by contract or because they have designed the product in a privacy-protective manner that minimizes the amount of personal data they need to access — all of which better protects the privacy of the personal data. Placing obligations to honour consumer rights requests on controllers minimises the data security and consumer privacy risks that would arise if processors were forced to respond to such requests and to access personal information that they would not otherwise need to access.

- *Improved efficiency in notification of data breaches*. BSA also supported the implementation of appropriate personal data breach notification requirements and congratulated the Australian Government on the successful implementation of the Notifiable Data Breach

[12] BSA 2020 Comments, p. 7.

scheme.[13] However, for the purposes of assigning responsibility in cases of multi-party breaches, the Act would benefit from a controller/processor distinction that clearly sets out the duties of each type of entity in the event of a breach. The Discussion Paper noted that, under the Privacy Act, the obligation to report an eligible data breach applies in relation to personal information held by an entity, which can lead to multiple entities having reporting obligations in relation to the same breach.[14] This situation, where a consumer receives multiple notifications for a single breach, can result in "notification fatigue" and erode the effectiveness of such notifications. The controller/processor distinction would address these issues by clearly allocating responsibilities for data breach notification. In doing so, it should recognise that if a processor suffers a data breach, it should be bound by contract to notify the controller, who, in turn, should notify data subjects, as soon as practicable, of a personal data breach involving the unauthorised acquisition of unencrypted or unredacted personal data that creates a material risk of identity theft or financial fraud. This would help entities more efficiently respond to requests by clearly delineating their different responsibilities. Moreover, this clear allocation would also address concerns that a processor may generally not be best placed to assess if a breach is notifiable, since the processor may be contractually prohibited from reviewing or analysing the personal data it is processing on behalf of the controller.

*Q2: If limitations in the Act's coverage makes full adoption of these concepts impractical, would partial adoption be beneficial? If yes, how could this occur without being overly complex?*

The small businesses exemption of enterprises with annual turnover of less than $3 million AUD under the Privacy Act introduces a challenge to effective implementation of the controller-processor distinction. For example, the Discussion Paper raises a hypothetical scenario of a small business controller engaging an APP entity as a processor, in which case neither entity would be subject to obligations to provide notice, seek consent, ensure security, or notify data breaches.[15]

We offer two views on how the AGD may approach this issue:

- *First, BSA supports the recommendation by the Office of the Australian Information Commissioner (**OAIC**) to remove the small business exemption*.[16] The exemption assumes that small businesses have a limited capacity to collect personal information, and hence present a reduced risk of privacy breaches. However, as noted by the OAIC, small businesses are now increasingly collecting, holding, and handling personal information in connection with their activities and to deliver their services.[17] BSA would like to reiterate our position that it is important to accord privacy obligations based on the entity's roles and responsibilities. Exempting small businesses, or indeed any other entity that acts as a controller, from their rightful controller obligations could undermine consumers' rights and present unnecessary and inadvertent risks to data security and privacy. Furthermore, the exemption is an "anomaly amongst international privacy laws",[18] and as such its removal would align Australia with international standards. This harmonisation would reduce compliance costs and facilitate trade, ultimately boosting economic growth.

[13] BSA 2020 Comments, p. 7-8.

[14] Discussion Paper (2021), p. 157.

[15] Discussion Paper (2021), p. 158.

[16] Privacy Act Review – Issues Paper, Submission by the OAIC, December 2020, https://www.ag.gov.au/sites/default/files/2021-01/office-of-the-australian-information-commissioner.PDF (**OAIC Submission (2020)**).

[17] OAIC Submission (2020), p. 60.

[18] OAIC Submission (2020), p. 60.

- *Second, in the event the small business exception is retained, the Act should not transfer the obligations of small-business controllers to their processors.* Doing so would only compound concerns around conflating these two distinct roles. Rather, the policy choice of whether to exempt small businesses or any other entity from the Privacy Act's obligations should be considered independent of the questions around obligations for processors. Indeed, if the small business exception is retained it would presumably apply both to small business controllers and to small business processors. As a result, in the hypothetical scenario poised by the Discussion Paper, in which a small business controller exempt from the Act engages a processor that is not a small business, the processor should still be subject to appropriate processor-focused obligations (detailed below). But the processor should not be required to take on the controller obligations for which the small business controller is exempt.

*Q3: If adopted, what obligations under the Act should processors have (record keeping, security, NDB), etc.?*

Both controllers and processors have important responsibilities and should be subject to strong obligations under a privacy law.

**Processors** should be assigned several types of obligations under a privacy law, namely:

- *Acting on behalf of a controlle*r. As a threshold matter, processors should be defined as entities that "process personal data on behalf of the controller." This ensures that a processor acts, in effect, as an agent of the controller and processes data on the controller's behalf.

- *Processing governed by contract*. The relationship between controllers and processors should be governed by a binding contract that sets out the obligations of both parties and requires that the processor only collect or process personal data on behalf of the controller as directed by the controller.

- *Data security*. Processors and controllers should both have strong obligations to safeguard consumers' personal data. For example, processors and controllers may both be required to employ reasonable and appropriate security measures, relative to the volume and sensitivity of the data, size, and nature of the business, and the cost of available tools.

- *Duty of confidentiality.* Processors may also be required to ensure that individuals processing data on behalf of the processor (e.g., the processor's employees) are subject to a duty of confidentiality with respect to such processing.

- *Notice of subprocessors*. Processors may also be required to notify a controller of its engagement of a subprocessor, including through a general authorisation agreed to by the controller and processor.

- *Assistance in responding to consumer rights requests*. Although the obligation to respond to consumer rights requests should be placed on controllers, as detailed below, processors may be appropriately required to provide reasonable assistance to controllers with respect to such requests. For example, a processor could be required to assist a controller by providing the controller with tools the controller can use to access, correct, or delete the controller's customers' information, or other reasonable assistance as may be practicable and appropriate in the context.

- *Determination of processor and controller is fact-based*. A privacy law may also appropriately recognise that determining whether an entity is acting as a controller or processor with respect to a specific processing of personal information is a fact-based determination that depends on the context in which the information is being or will be processed. If a processor

begins, alone or jointly with others, determining the purposes and means of the processing of personal data, it becomes a controller with respect to such processing. This helps to ensure that if an entity undertakes a processing activity with the intent to act as a processor, but begins determining the means and purposes of the processing (e.g., by using it for its own independent purposes), the entity is no longer treated as a processor under the Act but instead takes on the obligations of a controller.

These obligations are consistent with the obligations imposed on processors by many leading data protection and privacy laws, including the GDPR which sets out similar obligations in Article 28.

**Controllers**, in contrast, should be assigned consumer-facing responsibilities, such as an obligation to obtain consent from individuals and the obligation to respond to consumer rights requests. This is because controllers often have the direct relationship with individual data subjects. For this reason, leading privacy laws worldwide impose consumer-facing obligations on controllers, but not on processors. For example, the GDPR places on controllers the obligation to honour consumer rights requests and the obligation to provide data subjects with certain information about their processing. Processors are not subject to those obligations under the GDPR and are instead only required to assist controllers in fulfilling certain obligations and to process data pursuant to the controller's instructions.

**In summary, BSA recommends implementing a clear distinction between data controllers and processors, such that consumer-facing obligations do *not* apply to processors.**

## Scope and Definition of "Personal Information"

BSA previously recommended maintaining the present definition of personal information in the Privacy Act.[19]

### *Definition of Personal Information*

BSA supports defining personal information as information that relates to an identified or identifiable consumer.[20] This approach does not focus exclusively on the source of the information, but rather on the relationship between the information and the relevant individual. 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. BSA accordingly supports the Discussion Paper's proposal to change "about" to "relates to" in this definition.

BSA also supports introducing a non-exhaustive list of the types of information that fall within the definition "personal information" and including a list of objective factors to assist APP entities in determining when information relates to an identified or identifiable consumer. Greater specificity as to the types of technical and inferred personal information that would be covered by the Act would give entities more certainty about their obligations, thus encouraging more targeted data protection practices.

[19] Privacy Act, Section 6, "***personal information*** means information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not."

[20] 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.

In implementing these proposals, we recommend that the AGD clearly specify that information is not personal information if it is not reasonably related to a specific individual. This is in line with the proposal in the Discussion Paper, which notes that the amended definition of personal information "*would not capture information where there is only an extremely remote or hypothetical risk of identification*". Accordingly, the recommendation to ensure that inferred information falls within the definition of personal information should only be implemented to the extent that such inferred information relates to an identifiable individual.

For example, the Discussion Paper proposes to list "location data" as one of the types of information that falls within the definition of "personal information". However, there is no definition for what "location data" comprises, which leaves this term ambiguously broad. Location data does not always equate to personal information in personal information protection regimes around the world; and if location data were to be listed as proposed by the Discussion Paper, we recommend that the focus be on precise geolocation information, e.g., GPS-level longitude and latitude data, to avoid unnecessarily expanding the scope of information that would be considered personal information.

**In summary, BSA recommends stating, in the definition of personal information, that information which presents only a remote or hypothetical risk of identifying a specific consumer would *not* be covered by the Privacy Act. BSA also recommends that location data, should it be listed as an example of personal information, be limited to precise geolocation information relating to an identifiable individual.**

### *De-Identified and Pseudonymised Information*

The Discussion Paper also raises important questions around when information will be excluded from the scope of the Act. Specifically, the Discussion Paper proposes requiring personal information to be made anonymous[21] before it is no longer subject to the Privacy Act. Under this proposal, the definition of "de-identification" would be removed, and a definition of "anonymous information" inserted in its place.[22] We understand that this proposal stems from concerns regarding the increased risk of re-identification due to the amount of data in circulation, facilitated by advances in technology.[23]

Rather than taking this approach, we support maintaining the Act's current approach, under which data is not subject to the Act if it is de-identified. As noted above, the Discussion Paper already recommends clarifying the scope of data that constitutes personal information — and is thus covered by the Act because it is related to an individual. The Discussion Paper also recognises that the Act currently recognises that personal information is not covered by the Act if it is "no longer about an identifiable individual or an individual who is ***reasonably*** identifiable" (emphasis added).[24] These two definitions work together to clearly set out when information is within the Act's scope and when it is not. This clear dividing line also helps to ensure that information that presents only a remote or hypothetical risk of identifying a specific consumer would *not* be covered by the Privacy Act, in line with our recommendation above on the definition of personal information**.**

At the same time, the Discussion Paper does not expressly address if pseudonymised information would be excluded from the Privacy Act.

Pseudonymisation involves processing personal information in a manner such that the information can no longer be attributed to a category without including other related materials. The

---

[21] Discussion Paper (2021), p. 30. The Discussion Paper defines "anonymisation" as "the process of irreversibly treating data so that no individual ***can be identified***, including by the holders of the data" (emphasis added).

[22] Discussion Paper (2021), p. 30.

[23] Discussion Paper (2021), p. 30.

[24] Discussion Paper (2021), p. 29.

pseudonymised information is then organized according to a randomly generated identifier that is not used in other datasets. As pseudonymised information can no longer be linked to a specific individual without other related materials, it addresses the risk of re-identification by malicious third parties. The GDPR specifically states that pseudonymisation of personal information can reduce risks to the relevant individuals and help controllers and processors meet their obligations.[25] The pseudonymised information also retains some value for purposes like scientific research, thus facilitating data innovation among businesses.

**BSA therefore recommends that the Act: (1) continue to recognise that de-identified information is not subject to the Act, and (2) expressly state that pseudonymised information falls within the definition of personal information and subject that information to less stringent requirements than those applied to personal information. The Act should also actively encourage companies to use pseudonymisation.**

## Legitimate Interests

While the Discussion Paper notes that many industry stakeholders proposed the GDPR's legitimate interest basis[26] as a lawful basis for handling personal information in Australia, it also notes criticism that there is uncertainty surrounding the "broad and flexible" definition of legitimate interest.[27] The Discussion Paper then goes on to propose a "fair and reasonable test", i.e., that APP entities' collection and handling of personal information must be fair and reasonable.

BSA supports the recognition of legitimate interests as a lawful basis for handling personal information. The legitimate interests basis is a well-established feature of personal information protection frameworks that aims to facilitate the use of personal information for innovative purposes where it may not be suitable or appropriate for the controller to obtain consent to legitimise collection of the information, while also ensuring that risks to the individual rights of the relevant individuals are appropriately taken into account.

Legitimate interests include processing personal information 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, the legitimate interests basis would provide companies the flexibility and regulatory certainty to process personal information for these purposes.

Moreover, by recognising additional bases for processing personal information 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. This also encourages companies to adopt a robust risk-based approach to handling personal information, instead of over-relying on the "notice and consent" model.

Recognition of legitimate interests also does not conflict with the proposed "fair and reasonable test". This is evident in many other privacy regimes. For example, the GDPR, which requires personal information to be processed lawfully, fairly, and in a transparent manner (and which the proposed "fair and reasonable test" is based on), also recognises that legitimate interests of the controller constitute

[25] GDPR, Recital 28.

[26] Article 6 of the GDPR provides six lawful bases for processing data, including where "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject".

[27] Discussion Paper (2021), p. 83.

a lawful basis for processing such data.[28] Even in consent-based frameworks like Singapore's Personal Data Protection Act 2012 (**PDPA**), where consent is the primary legal basis for collecting and processing personal information, legitimate interests has been recognised as a basis for processing.[29]

The Discussion Paper's main criticism of legitimate interests — that the definition of legitimate interests is broad and flexible — could be overcome by having guidelines, factors, and checklists to assist entities in using this basis for processing personal information, while taking into account the interests and rights of the relevant individuals. A possible reference point in this regard is the PDPA, which sets out a voluntary but comprehensive checklist to guide companies in assessing whether they may rely on the PDPA's legitimate interests exception.[30]

**BSA recommends recognising legitimate interests as a lawful basis for the processing of personal information. BSA also recommends setting out guidelines, factors, and checklists to assist companies in understanding what would constitute a "fair and reasonable test" in order to rely upon legitimate interests, and how these interests should be balanced against the interests and rights of data subjects.**

## Security and Destruction of Personal Information

The Discussion Paper recognises the importance of securing personal information and raises several questions about the existing security and destruction requirements for APP entities. These include potentially amending APP 11.2 to require APP entities to take *all* reasonable steps to destroy or to *anonymise* personal information when it is no longer needed or required.[31]

We are concerned that changing the current obligation from taking "such reasonable steps as are reasonable in the circumstances" to "all reasonable steps" creates more ambiguity for businesses – not less. (That ambiguity is compounded by changing the standard to be met from "de-identification" of the information to "anonymisation," as explained above.) Most fundamentally, this change does not provide entities with guidance about what steps they are required to take, and which steps will be considered reasonable. For example, where personal information is a phone number, it is not clear whether deleting the last 4 digits of the phone number could satisfy the "all reasonable steps" requirement or whether deleting the entire phone number would be necessary.

Rather than amending the APP to require that "all" reasonable steps be taken, we encourage the Australian Government to publish guidance addressing what actions constitute reasonable steps for destruction and de-identification. This will help entities to meet their obligations and help them to identify ways to destroy or de-identify personal information that is no longer needed. Absent such guidance, entities may be required to put in place onerous and costly information destruction technical capabilities and equipment where the entity does not already have such capabilities or equipment.

[28] GDPR, Articles 5(1)(a) and 6(1)(f).

[29] PDPA, First Schedule Part 3 – Legitimate Interests.

[30] Assessment Checklist for Legitimate Interests Exception, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Annex-C--Assessment-Checklist-for-Legitimate-Interests-Exception-1-Feb-2021.pdf?la=en.

[31] Discussion Paper (2021), p. 148.

## Overseas Data Flows

The Discussion Paper proposes to introduce: (1) a mechanism to prescribe countries and certification schemes under APP 8.2(a);[32] and (2) standard contractual clauses (**SCCs**) for the cross-border transfer of personal information.[33]

In line with our earlier recommendation, BSA encourages the Australian Government to recognise different data transfer mechanisms which can meet the requirements imposed by the Act and support the accountability model for international data transfers. These include the APEC CBPR and PRP,[34] as well as mutual recognition arrangements, such as adequacy with the GDPR. Recognising these mechanisms would align the Act with global best practices and give entities the flexibility to determine which mechanisms will be better suited for each situation. These mechanisms are also incorporated in other data protection frameworks to promote cross-border data flows.

We also urge the Australian Government to refrain from creating new data transfer mechanisms solely for use by entities transferring data to and from Australia as such measures would not encourage the widespread use of interoperable mechanisms to facilitate responsible data transfers. For example, if the proposed SCCs are not interoperable with other similar standard contractual clauses, they would impose operational and compliance challenges for entities operating in multiple jurisdictions. As such, BSA recommends that any new Australian-specific data transfer mechanisms should remain voluntary and be interoperable with other global schemes to help further industry participation and ensure meaningful protections for consumers.

BSA also supports retaining the following exceptions:

- APP 8.2(a) for recipients subject to "at least substantially similar" protection to the APPs, as the exception provides a straightforward path for entities transferring personal information to jurisdictions offering robust and enforceable privacy regimes, and enhances flexibility while preserving consumer protections.

- APP 8.2(b) on informed consent[35], as removing the informed consent exception would increase the regulatory burden on entities seeking to transfer personal information overseas and on entities which have relied on the exception in the past.

**The Discussion Paper also proposes to strengthen the transparency requirements in relation to potential overseas disclosures by including information such as the destination countries that personal information may be disclosed to, as well as the specific personal information that may be disclosed overseas.** While improving the transparency of data transfer processes is an important prerogative, such requirements might not materially impact or enhance consumers' understanding of how these transfers might affect the processing and protection of their personal information. Disclosing transfer destination countries, for example, does not provide consumers any actionable information about the risks of processing due to the existence of numerous other factors, such as differences in how national laws are applied *in practice*, based on the type of information being transferred, the nature of the service, and legal and procedural limits on access to information that may be non-public given their use in law enforcement and national security contexts. **In this regard, we caution against adopting Proposal 22.4 in the Discussion Paper.**

---

[32] Discussion Paper (2021), pp. 160-161.

[33] Discussion Paper (2021), pp 161-162.

[34] See http://cbprs.org/ and http://cbprs.org/business/.

[35] Schedule 1, APP 8.2(b) of the Privacy Act states that APP 8.1 will not apply to the disclosure if: (1) the APP entity expressly informs the individual that if he or she consents to the disclosure of the information; and (2): after being so informed, the individual consents to the disclosure.

## Direct Right of Action and Statutory Tort for Invasion of Privacy

The Discussion Paper considers creating a direct right of action for breaches of privacy obligations.[36] This would allow individuals or groups of individuals to initiate an action in the Federal Court or Federal Circuit Court where an APP entity breaches its privacy obligations. Notably, the OAIC may, at the request of the court, appear as amicus curiae to provide expert evidence.[37] Additionally, the Discussion Paper also considers creating a statutory tort for invasion of privacy including intrusion upon seclusion and misuse of private information as recommended by the ALRC Report 123.[38]

BSA does *not* support the introduction of a direct right of action or a statutory tort for invasion of privacy. The enforcement of a privacy law should be agency-led, as agencies can create a consistent body of enforcement efforts demonstrating how the agency will apply privacy rights and obligations in a variety of contexts, particularly when combined with informal or formal guidance interpreting the privacy law. This approach provides much-needed clarity for consumers and entities as to how the rights and obligations under the privacy law will be applied. An agency like the OAIC is well-placed to provide such clarity.

In contrast, a direct right of action and a statutory tort would encourage enforcement by way of private litigation; and 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 individuals and entities wanting to understand their rights and obligations in advance. As such, even if a direct right of action is eventually introduced, the enforcing agency should always be called upon to provide expert views during the proceedings to enhance regulatory coherence. Further, if both direct rights of action and a statutory tort for invasion of privacy are introduced, potential litigants may bring multiple claims for the same breach, potentially resulting in frivolous and resource-wasteful litigation while offering the litigants two opportunities to sue for the same alleged violation.

The experience of the implementation of the California Consumer Privacy Act (**CCPA**) is illustrative of the potential flurry of litigation that could ensue if a direct right of action and/or a statutory tort were to be introduced in Australia's privacy regime. The CCPA provides consumers a private right of action to sue, as individuals or a class, businesses for certain data breach incidents and potentially recover up to $750 USD in statutory damages "per consumer per incident or actual damages, whichever is greater". Despite the right being narrowly scoped, in the short seven months after the CCPA went into effect on January 1, 2020, around 50 lawsuits were filed invoking the CCPA.[39] Plaintiffs challenged the limits of the CCPA's private right of action in every way they could: the plaintiffs sought to apply the CCPA retroactively or beyond its geographic limits; the plaintiffs ignored that the CCPA limits the kinds of violations on which the private right of action can be based; and the plaintiffs sought to use the CCPA as the standard of care for other statutory or common law claims.[40] The introduction of a direct right of action or a statutory tort for invasion of privacy in Australia could also result in similar unintended consequences even if such measures were appropriately and narrowly framed.

**BSA recommends that a direct right of action and statutory tort *not be* introduced into the Privacy Act and that the common law should be allowed to develop as required. If a direct right of action is introduced, BSA suggests that the participation of the enforcing agency in the court proceedings should be made mandatory, so as to enhance regulatory coherence.**

---

[36] Discussion Paper (2021), p. 186.

[37] Discussion Paper (2021), p. 189.

[38] Discussion Paper (2021), p. 191.

[39] Holland & Knight LLP, Holland & Knight Alert: Litigating the CCPA in Court, 22 July 2020, https://www.hklaw.com/en/insights/publications/2020/07/litigating-the-ccpa-in-court.

[40] Morrison & Foerster LLP, Privacy Litigation 2020 Year in Review: CCPA Litigation, 6 January 2021, https://www.mofo.com/resources/insights/210106-privacy-litigation-2020-year-review.html.

## Treatment of Employee Data

BSA recommends that the employee records exemption should be retained but recognises that modifications may be appropriate to allow better protection of employee records while retaining the flexibility employers need to administer the employment relationship. Removing the exemption entirely, which would require all APP entities to comply with the Act in relation to their handling of personal information of employees and former employees, would create significant concerns. As the Discussion Paper notes, several obligations in the Act may be inappropriate or irrelevant in the employment context and could inadvertently limit the ability of employers to undertake sensitive managerial processes including performance management and disciplinary investigations. **We support retaining the employee records exception and ensuring any modifications to that exception recognise the unique aspects of the employer-employee relationship.**

## Individual Rights Requests

We support including important consumer rights in personal information protection laws, including the rights to object and erase their personal information and data portability. However, these rights must be implemented in a manner that does not raise new privacy and security concerns. Also, it is important to reiterate that controllers, and not processors, should be the recipients of and responsible for implementing requests regarding consumer privacy rights. In considering the rights of individuals under the Act, we make the following recommendations:

- *Right to Object and Portability (Chapter 14)*: BSA recommends that any right to object should be qualified and should not be absolute, as information may still need to be processed by the APP entity to comply with laws, to carry out billing, to guard against fraud, etc. We recommend incorporating flexibilities and limitations,[41] including the scope of processing to which the right applies so that the right to object is qualified and not absolute.

- *Right to Erasure of Personal Information (Chapter 15)*: The proposed section 15.1 permits erasure of sensitive information and erasure requested by parents, which seem to go beyond the consent-based revocation/erasure requests contemplated by GDPR Articles 17.1(b) and (c). To the extent that the right to erasure is adopted, we recommend creating a right that is interoperable with the GDPR and focuses on concerns based on revocation of consent and other limited grounds. Such right to erasure should also recognise exceptions for circumstances in which the entity cannot comply with such a request, including as a result of legislation or contract.

- *Direct Marketing, Targeted Advertising and Profiling (Chapter 16)*: The Discussion Paper states that the current limited right to opt out of receiving direct marketing communications could be replaced with an unqualified right to object to the collection, use, and disclosure of personal information for the purposes of direct marketing. BSA recommends ensuring that this obligation is placed on controllers, which are the only entities positioned to honour such requests. To the extent the controller/processor distinction is not adopted in the Act, this result could also be achieved by creating a clear exception for service providers/intermediaries that disseminate such communications on behalf of the direct marketing entity.

For completeness, the Discussion Paper also seeks feedback on whether regulated entities should be required to: (1) enable pro-privacy settings by default, or (2) make privacy settings easily accessible to individual.[42] In this regard, BSA recommends that the requirements be limited to ensuring that privacy settings are clear and easy to access, and therefore Option 2 should be adopted.

---

[41] For example, see GDPR Article 21.

[42] Discussion Paper (2021), p. 98.

## Conclusion

We thank the AGD for the opportunity to comment on the review of the Act and appreciate AGD's kind consideration of our above comments. We hope that our concerns and recommendations will assist in the development of a rigorous privacy regime, which enhances privacy protections while providing regulatory certainty for businesses. We, and our members, would be happy to meet with the AGD to discuss our submission and would welcome the AGD's continued engagement on this important matter.

Please do not hesitate to contact me if you have any questions regarding this submission or if I can be of further assistance.

Sincerely,

Tham Shen Hong
Manager, Policy – APAC

# How Enterprise Software Empowers Businesses in a Data-Driven Economy

## B2B software enables business customers to do what they do best—faster, smarter, and more efficiently.

## Enterprise Software Supports Businesses' Operations

Enterprise software—or business-to-business (B2B) software—**enables** the operations of other companies. It helps organizations of all sizes and across all industries operate more safely and efficiently, enhance product and service development, and increase opportunities to innovate and grow.

The enterprise software industry supports a wide range of organizations across the world, including SMEs and large companies; local and central governments; hospitals, schools, and universities; and non-profits. By **offering trusted and responsible software solutions** to support their business clients' data-processing needs, enterprise software companies enable other organizations to service their own customers in turn.


Enterprise software optimizes the use of digital technology to support and improve business operations, empowering other companies to focus on what they do best, such as R&D and product design.

**In Europe**, almost **80 percent of large companies** and **35 percent of SMEs** use information-sharing software.[1]

## Enterprise Software Helps Businesses Benefit From Digital Transformation

Organizations in every sector of the economy increasingly rely on cutting-edge software to **run, facilitate, improve, and optimize their operations** every single day. Governments, public administrations, schools, and hospitals are also increasingly adopting these tools. Enterprise software underpins human resources and payroll operations; billing and financial transactions; research and development; product design; workforce collaboration, communication, and messaging; customer relations; and logistics and supply-chain management, among many other business services.

**38 percent** of small businesses in the **United States** cited increased sales and revenue as a benefit associated with using digital tools.[2]

**Australian businesses** are using more cloud than ever—**42 percent of businesses** across 2017–2018, up from 31 percent in 2015–2016.[3]

In times of crisis, such as the global outbreak of COVID-19, enterprise software tools help coordinate public health safety responses, maintain essential services, and support economic continuity.

## ENTERPRISE (B2B) SOFTWARE PROVIDES CLIENT SOLUTIONS THAT:

**Operate and Optimize Business Services**
(including responsibly handling and moving information globally)

**Protect and Secure Data and Business Information**
(including providing strong, accountable privacy and security safeguards)

**Innovate and Expand Beyond Existing Capabilities**
(by using cognitive solutions such as analytics and artificial intelligence to better address customers' needs)

[1] EU DESI Index 2020, https://ec.europa.eu/digital-single-market/en/digital-economy-and-society-index-desi.

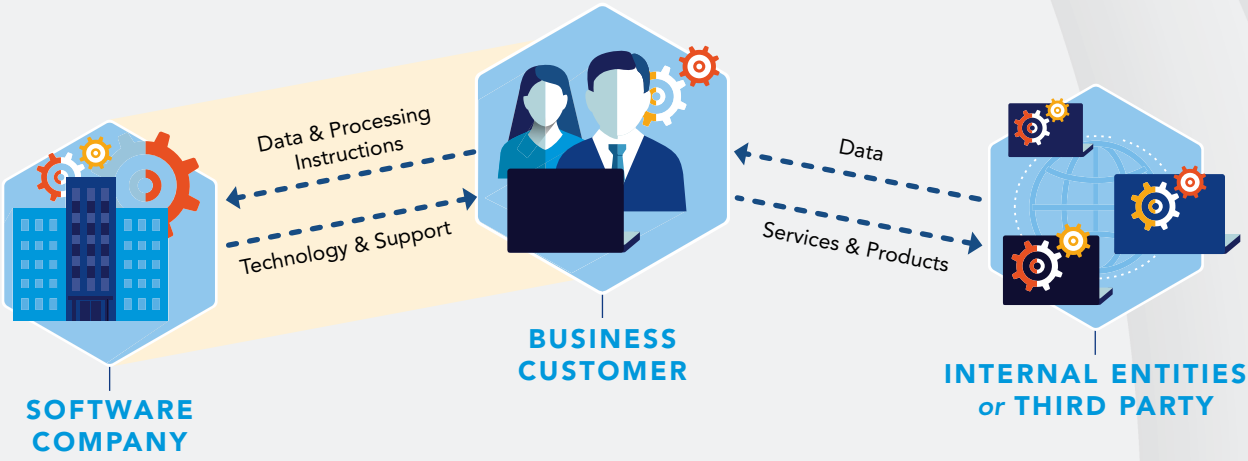
[2] https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/connected-small-businesses.html.

[3] Characteristics of Australian Business, https://www.abs.gov.au/statistics/industry/technology-and-innovation/characteristics-australian-business/2017-18.

# Enterprise Software Is Built on Transparency and Trust

Enterprise software companies and their business customers negotiate their relationship in contracts and licensing agreements to ensure they best address their clients' individual needs. **Enterprise software companies monetize their technologies and not the data of their customers.**

Enterprise software services, such as cloud computing, are used primarily for business-to-business purposes and are not consumer facing. **The business customers control their data and direct how it will be used.** Enterprise software companies do not have unfettered access to the data stored in their cloud infrastructure or service. Access and use of such data is reserved for the benefit and sole purpose of their customers.




**Enterprise software companies operate under strong existing legislative requirements of data handling.** Across the world, legal obligations often include accountability measures and technical safeguards that ensure enterprise software companies provide robust assurances of trust for their customers. Enterprise software companies also develop innovative, tailored, or customizable solutions for clients that are highly regulated, for example, in the health, financial, automotive, aeronautic, and telecom sectors and the semiconductor industry.[4]

For instance, machine learning solutions can use data gathered across countries to create fraud detection systems in the financial sector.

**Enterprise software helps reduce legal and operational risks for business customers** who can be confident they are using tried and tested software products, with appropriate remedies and support, without having to develop their own software in-house. Enterprise software companies also often provide tools to facilitate their customers' compliance, for instance on privacy, consumer protection, cybersecurity, anti-money laundering, or energy efficiency.

[4] See Cross-Border Data Flows: Enabling Local Economies and Driving E-Commerce, https://www.globaldataalliance.org/downloads/WTOEventSummary20200702.pdf.

# How to Create a Successful, Responsible, Software-Enabled Economy

## STRONG PRIVACY PROTECTIONS

Privacy is essential to building trust. Software-enabled business operations increasingly rely on data—and, in some cases, personal data—to function. As a result, data protection frameworks that create a user-centric approach to privacy must ensure the use of personal data is clear, transparent, and consistent with customers' expectations. Privacy laws should create robust obligations for all companies and organizations that handle individuals' personal data. This would ensure companies act responsibly while being able to pursue legitimate business interests.

## CYBERSECURITY

Software innovation continues to connect people across the world. These online connections create efficiencies and spur economic growth, but they also create vulnerabilities that bad actors can exploit if the proper security measures are not in place. Addressing cybersecurity challenges requires innovative tools and practices to defend the integrity, confidentiality, and resilience of the connected ecosystem. One important tool is the ability to use the strongest available encryption technology when appropriate.

## CROSS-BORDER DATA FLOWS

Cross-border data flows are necessary for companies to operate globally; leverage their resources and footprint across locations; innovate; and provide services to their customers, across sectors and geographies. For enterprise software companies and their business customers, the ability to transfer, and process, data globally is pivotal in ensuring the quality, reliability, security, personalization, and efficiency of service.

## RISK-BASED AND TECHNOLOGY-NEUTRAL APPROACH

Software technologies evolve every day, pushing the boundaries of the benefits that technology can bring to organizations and people. Given the fast-paced nature of this industry and its adoption by customers, laws and regulations should strive to provide legal certainty, be outcome-based, and adopt a risk-based and technology-neutral approach, building on legal frameworks that already apply. Any new policy should set clear compliance goals and enable companies to adapt their practices and safeguards to the best-suited approach given their business model, the nature of their activity, their position in the value chain when contracted by others, and their risk profile vis-à-vis the established objective.

## INTERNATIONAL CONVERGENCE

The value of the data-driven economy is in the ability of companies to operate across borders, reach new markets, and service customers regardless of location. Building on each region's own legal and cultural legacy, convergence of rules on privacy, cybersecurity, or data governance and compatibility of mechanisms play a critical role in growing cross-border business that increasingly rely on enterprise software around the world.

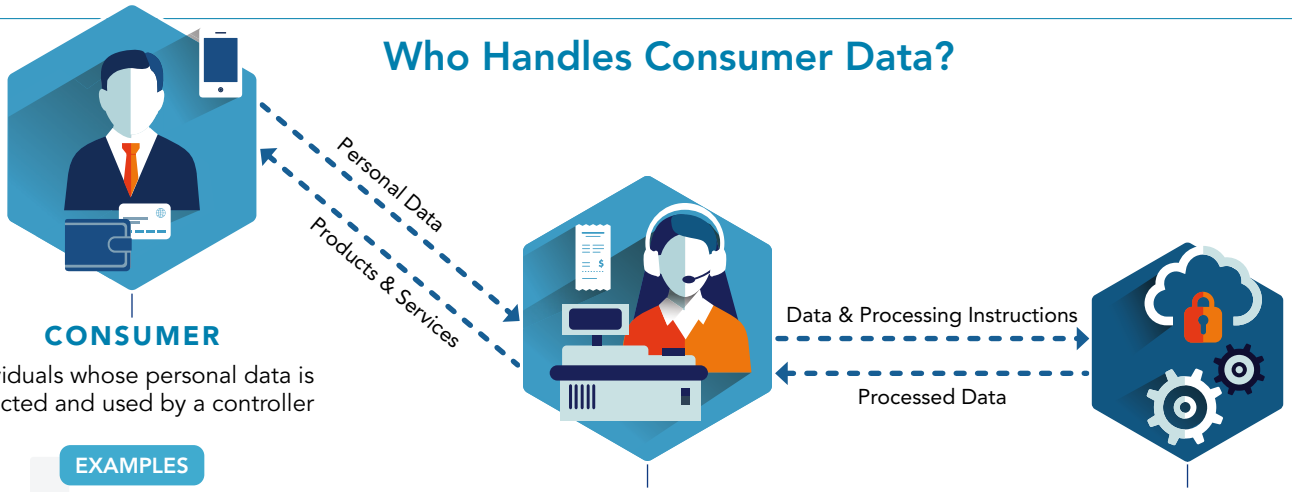
# The Global Standard: Distinguishing Between Controllers and Processors in Privacy Legislation

Comprehensive privacy legislation must create strong obligations for all companies that handle consumer data. These obligations will only be strong enough to protect consumer privacy and instill trust, though, if they reflect how a company interacts with consumer data.

Privacy laws worldwide distinguish between two types of companies: (1) businesses that decide *how* and *why* to collect consumer data, which act as **controllers** of that data and (2) businesses that process the data on *behalf of* another company, which act as **processors** of that data

This fundamental distinction is critical to a host of global privacy laws, including the European Union's General Data Protection Regulation ("GDPR") and the California Consumer Privacy Act ("CCPA"). Both types of businesses have important responsibilities and obligations, which should be set out in any legislation.

## Who Handles Consumer Data?




### CONSUMER

Individuals whose personal data is collected and used by a controller

**EXAMPLES**

Consumers who shop at retail stores, buy products online, or share information on social media platforms.

**CONSUMERS SHOULD HAVE THE RIGHT TO:**

- **Know** what type of data a controller collects — and why
- **Say no,** and opt out of broad types of use, not just sale
- **Access** information about them
- **Correct** that information
- **Delete** that information
- Have their data **securely protected**
- Have their data used **consistent with their expectations**

### CONTROLLER

Decides whether and how to collect data from consumers, and the purposes for which that data is used

**EXAMPLES**

Companies that interact directly with consumers, such as hotels, banks, retail stores, travel agencies, and consumer-facing technology providers.

**CONTROLLERS ARE RESPONSIBLE FOR:**

Obtaining any consent needed to process a consumer's data

Responding to consumer requests for access, correction, or deletion

Using data consistent with the consumers' expectation

### PROCESSOR

Processes data on behalf of a controller, pursuant to the controller's instructions

**EXAMPLES**

Companies that provide business-to-business products like cloud computing, and vendors like printers, couriers, and others that process data at the direction of another company.

**PROCESSORS ARE RESPONSIBLE FOR:**

Processing data consistent with a controller's instructions

Adopting appropriate safeguards designed to protect data security

Controllers and processors should have role-dependent responsibilities to ensure consumers' privacy and security are protected.

## Privacy Laws Worldwide Distinguish Between Controllers and Processors

Privacy laws worldwide reflect the basic distinction between companies that decide to collect and use data about individuals and companies that only process such data.

| Companies that decide how and why to collect consumer data. | Companies that process consumer data at the direction of others. |
|---|---|
| **GDPR: Controllers** Determine the "purposes and means" of processing. | **GDPR: Processors** Handle personal data "on behalf of" a controller. |
| **CCPA: Businesses** Determine the "purposes and means" of processing. | **CCPA: Service Providers** Handle personal information "on behalf of" businesses. |

This distinction is crucial to a host of privacy laws beyond the GDPR and CCPA. 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.

**EXAMPLE**

A business contracts with a printing company to create invitations to an event. The business gives the printing company the names and addresses of the invitees from its contact database, which the printer uses to address the invitations and envelopes. The business then sends out the invitations.

The business is the controller of the personal data processed in connection with the invitations. The business decides the purposes for which the personal data is processed (to send individually-addressed invitations) and the means of the processing (mail merging the personal data using the invitees' addresses). The printing company is the processor handling the personal data pursuant to the business's instructions. The printing company cannot sell the data or use it for other purposes, such as marketing. If the printing company disregarded those limits and used the data for its own purposes, it would become a controller and be subject to all obligations imposed on a controller.

## Why Is the Distinction Between Controllers and Processors Important to Protecting Consumer Privacy?

Distinguishing between controllers and processors ensures that privacy laws impose obligations that reflect a company's role in handling consumer data. This helps safeguard consumer privacy without inadvertently creating new privacy or security risks.

**Data Security.** Controllers and processors should both have strong obligations to safeguard consumer data.

- Placing this obligation on both types of companies ensures consumer data is protected.
- Controllers and processors should both employ reasonable and appropriate security measures, relative to the volume and sensitivity of the data, size, and nature of the business, and the cost of available tools.

**Consumer Rights Requests.** Responding to important 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, laws like the GDPR and CCPA require controllers to respond to consumer rights requests. Moreover, 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.
- Processors, in contrast, often do not know the content of the data they process, and may be contractually prohibited from looking at it. It is not appropriate for processors to respond directly to a consumer's request—which creates both security risks (by providing data to consumers they do not know) and privacy risks (by looking at data they otherwise would not). Processors should instead provide controllers with tools the controller can use to collect data needed to respond to a consumer's request.