



10 April 2023

BSA COMMENTS ON THE PRIVACY ACT REVIEW REPORT 2022

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's (**AGD**) Privacy Act Review Report 2022 (**Report**).²

BSA is the leading advocate for the global software industry. BSA members create technology solutions that power other businesses, including cloud storage services, customer relationship management software, human resources management programs, identity management services, security solutions, and collaboration software. Our members have made significant investments in Australia, and we are proud that many Australian companies and organisations continue to rely on our members' products and services to do business and support Australia's economy. BSA members recognise that companies must earn their consumers' trust and act responsibly with their personal information.

BSA has participated in many privacy-related consultations in Australia.³ We are encouraged that our submission on the AGD's Privacy Act Discussion Paper in 2021 (**Discussion Paper**)⁴ was referenced throughout the Report and we appreciate the opportunity to provide further comments to support the AGD's continued efforts to revise and enhance the Privacy Act 1988 (**the Act**) and ensure it is fit for purpose for a modern Australia. BSA supports many proposals in the Report, particularly the proposal to implement a clear distinction between controllers and processors.⁵ Clearly distinguishing between these roles will improve privacy protections for consumers and increase interoperability with leading personal data protection laws worldwide. Our recommendations, described in further detail below, focus on eight areas:

- Implementing a clear distinction between controllers and processors;
- Retaining the employee records exemption to reflect the distinct nature of the employer/employee relationship;
- Ensuring that the Act's treatment of international data transfers enhances cross-border transfers with Australia;

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

² Privacy Act Review Report 2022, February 2023, https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf (**Report 2023**).

³ See: BSA Comments on Australia Online Privacy Bill, December 2021, <https://www.bsa.org/policy-filings/australia-bsa-comments-on-australian-online-privacy-bill>; BSA Comments on Review of Australia Privacy Act, January 2022, <https://www.bsa.org/policy-filings/australia-bsa-comments-on-review-of-australia-privacy-act-1988>; BSA Comments on Privacy Legislation Amendment Bill, October 2022, <https://www.bsa.org/policy-filings/australia-bsa-comments-on-privacy-legislation-amendment-bill>.

⁴ BSA Comments on Review of the Australian Privacy Act 1988, January 2022, <https://www.bsa.org/policy-filings/australia-bsa-comments-on-review-of-australia-privacy-act-1988> (**BSA 2022 Comments**).

⁵ Report (2023), Proposal 22.1.

- Focusing enforcement on existing mechanisms, without creating a direct right of action for interferences with privacy or a new statutory tort for serious invasions of privacy.
- Ensuring consistent regulatory enforcement of a “fair and reasonable” test;
- Including a legitimate interests basis for processing in the Act;
- Aligning potential new provisions on automated decision-making with existing laws in other jurisdictions; and
- Specifying how Section 13G’s penalties will apply to “serious” violations of the Act.

Our comments also provide recommendations on several other aspects of the Report, including on proposals to reform the scope and application of the Act and its substantive protections including consent and notice obligations.

Controller-Processor Distinction (Proposal 22.1)

BSA strongly supports the introduction of a controller-processor distinction into the Act.⁶ This distinction is fundamental to privacy and data protection laws worldwide. Adopting this distinction in the Act will enhance its protections for consumers and improve clarity for businesses.

As the Report recognises, there are significant benefits to distinguishing between controllers and processors under the Act. Adopting the distinction between controllers and processors will align the Act with privacy laws globally, including the European Union’s General Data Protection Regulation (**GDPR**),⁷ California’s Consumer Privacy Act (**CCPA**),⁸ Japan’s Act on the Protection of Personal Information (**APPI**),⁹ and Singapore’s Personal Data Protection Act (**PDPA**).¹⁰ This alignment will help Australian entities understand how their obligations under the Act map to their obligations under data protection laws in other major jurisdictions.¹¹ Clearly distinguishing between the roles of controllers and processors — and assigning distinct obligations to both types of entities — also improves consumer protection and enhances regulatory certainty for businesses. The Report notes that distinguishing between controllers and processors will “clarify consent obligations and assist with clarifying obligations in relation to any new individual rights (such as a right to erasure) that may be introduced following this review”, and “help entities more effectively respond to data breaches.”¹²

We applaud the AGD for recognising the importance of the controller-processor distinction. Our recommendations focus on two key issues as the AGD implements this distinction in the Act:

Definitions: We agree with the Report that the definitions of controllers and processors will need to be carefully considered in at least two ways.

First: Australia should adopt definitions of controllers and processors that align with definitions already used in other important privacy laws. Under the GDPR, for example, controllers are defined as an entity that “alone, or jointly with others, determines the purposes and means of processing personal data.” Processors are defined as an entity that “processes personal data on behalf of the controller.”¹³ The GDPR, like many other privacy and data protection laws globally, clearly distinguishes between companies that decide how and why to

⁶ Report (2023), p. 233.

⁷ European Union General Data Protection Regulation, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>.

⁸ California Consumer Privacy Act of 2018, http://leginfo.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

⁹ Amended Act on the Protection of Personal Information (English), https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf.

¹⁰ Personal Data Protection Act 2012, <https://sso.agc.gov.sg/Act/PDPA2012>.

¹¹ Report (2023), p. 231.

¹² Report (2023), p. 231.

¹³ GDPR, Article 4.

collect an individual's personal data — i.e., those determining the purpose and means of processing that data — from companies that act on behalf of others.¹⁴ We recommend Australia adopt the same formulation and define controllers as companies that alone or jointly with others determine the purposes and means of processing personal information and processors as entities that process personal data on behalf of a controller.

Second: The Act should clearly recognise that determining whether an entity is acting as a controller or processor is fact-based and context specific. A single company may act as a controller for some of its products and services (i.e., consumer-facing products) and as a processor for others (i.e., business-to-business services). Such a company should be subject to obligations the Act places on controllers when it acts as a controller and subject to obligations the Act places on processors when it acts as a processor. We recommend expressly stating this in the Act. For example, language could draw from state privacy laws in the United States which recognise that determining whether an entity is acting as a controller or processor with respect to 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.¹⁵ This language also makes clear that if a processor begins determining the purposes and means of processing personal data (e.g., by using the data for its own independent purposes), it is no longer treated as a processor under the Act but instead takes on the obligations of a controller.

Obligations for Controllers and Processors: Controllers and processors should be subject to distinct obligations under the Act. The Report sets out a table of proposed obligations for controllers and processors mapped to the Australian Privacy Principles (**APP**).¹⁶ We support the chart's recognition that different APPs will be appropriate for controllers and processors, based on their different roles. We make two recommendations as the AGD implements these obligations.

First: Ensure that consumer-facing responsibilities are assigned to controllers rather than processors. Privacy laws worldwide place consumer-facing obligations like obtaining consent from individuals and responding to consumer rights requests on controllers. This reflects the fact that controllers are best positioned to respond to consumers because they are the entities that decide how and why to collect a consumer's personal information. Processors should be subject to other obligations, such as requirements to safeguard personal information and to only process personal information on behalf of the controller and pursuant to its instructions. Although the Report's chart reflects these separate roles, it nevertheless appears to place several consumer-facing obligations on processors. For example, the Report contemplates that processors will be subject to APP 1 (open and transparent management of personal information), but APP 1.2 and 1.6 include consumer-facing obligations that are not suited to processors. Notably, APP 1.2 requires an entity to implement practices, procedures, and systems that will enable it to deal with inquiries or complaints from individuals, whereas APP 1.6 requires an entity to provide individuals with a copy of its APP Privacy Policy in a particular form that an individual requests. We recommend introducing amendments that recognise consumer-facing transparency requirements do not apply to processors.

Second: Ensure that processor obligations under the notifiable data breaches (NDB) scheme reflect processors' roles. The Report suggests a processor must notify both the

¹⁴ Controllers and Processors: A Longstanding Distinction in Privacy, October 2022, <https://www.bsa.org/files/policy-filings/10122022controllerprodistinction.pdf> and appended to this submission.

¹⁵ See, e.g., Colorado Privacy Act Sec. 6-1-1305(7), available at https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf, Connecticut Data Privacy Act Sec. 7(d), available at <https://www.cga.ct.gov/2022/ACT/PA/PDF/2022PA-00015-R00SB-00006-PA.PDF>, and Virginia Consumer Data Protection Act Sec. 59.1-579.D, available at <https://law.lis.virginia.gov/vacode/title59.1/chapter53/section59.1-579/>.

¹⁶ Report (2023), p. 233. See also the Australian Privacy Principles (Schedule 1 to the Privacy Act), <https://www.legislation.gov.au/Details/C2022C00361>.

controller and the Information Commissioner (**IC**) where there is a data breach.¹⁷ Specifically, the Report proposes that a processor would be “required to prepare a statement on the breach and provide a copy of that statement to the IC unless the breach has already been reported by the relevant controller.”¹⁸ Moreover, if “neither processor nor controller notifies the IC, both may be in breach of the scheme’s requirements.”¹⁹

This formulation is not consistent with the role of processors and complicates the allocation of responsibilities between controllers and processors when there is a data breach. For example, the Report proposes that both controllers and processors would provide the IC with a statement that describes the eligible data breach, the kinds of information concerned, and recommendations about steps that individuals should take in response. Processors, however, often have limited insight into this information and are therefore not well-situated to provide information the IC seeks. In many cases, a data processor’s access to and knowledge of personal information collected by its enterprise customers are limited by the privacy and security controls built into its products and enforced by contractual terms between the processor and the data controllers that are its customers. As a result, a processor may lack access to the facts needed to determine if an incident rises to the level of an eligible data breach. Moreover, the processor will often lack insight into the type of information that was compromised, including whether such data included personal information, and the steps individuals should take in response.

BSA agrees that processors should be required to report breaches to a controller. However, the controller is best situated to provide all the necessary information to the IC. We therefore recommend the Act not require processors to report breaches directly to the IC. Instead, the Act should require processors to report breaches to a controller and require the controller to report to the IC and to data subjects.

Recommendation: The Act should implement a clear distinction between controllers and processors that: (1) adopts definitions of controllers and processors modelled on the GDPR’s definitions, which have been incorporated into data protection and privacy laws worldwide; (2) recognises that determining if an entity is acting as a controller or a processor is fact-based and context-specific; (3) avoids placing consumer-facing obligations on processors; and (4) appropriately reflects the role of processors in the data breach notification scheme.

Employee Records Exemption (Proposal 7.1)

BSA supports retaining the employee records exemption 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. We therefore support the Report’s recommendation to conduct further consultations about how to enhance privacy protections for private sector employees while ensuring that employers have adequate flexibility to collect, use, and disclose employees’ information to administer the employment relationship.²⁰

Importantly, the Report does *not* propose to do away with the employee records exemption. 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. For example, 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. As highlighted in the Report, a business may be “negatively impacted by the application of APPs 3, 6, 12 and 13 along with pro-privacy defaults, restricted and prohibited practices and any new rights to object

¹⁷ Report (2023), p. 233 and 292.

¹⁸ Report (2023), p. 292.

¹⁹ Report (2023), p. 292.

²⁰ Report (2023), p. 70-71.

and erasure.”²¹ The Report goes on to note that rights to request access or correction under these APPs “could discourage referees from giving a full and frank reference, and employers from conducting investigations or managing employee performance.”

Recommendation: To the extent that the employee records exception is modified, businesses should not be subject to consumer-facing obligations vis-a-vis their employees (e.g., obligations to respond to requests for access or correction, or consent requirements), which raise distinct concerns in the context of employment relationships. We welcome further consultations on these important issues to ensure that any modifications recognise the unique aspects of the employer-employee relationship.

International Data Transfers (Proposals 23.1–23.6)

We support the Report’s objective of ensuring that any changes to the Act’s treatment of international data transfers enhance cross-border data transfers with Australia as a trusted trading partner and create economic benefits for Australian businesses and the economy.²² 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 drive innovation, increase employment, and build economies.

We offer recommendations on implementing five proposals that affect the Act’s application to international data transfers:

Extraterritorial Application (Proposal 23.1)

The Report recommends conducting additional consultations on the potential to require an “Australian link” to apply the Act to foreign organisations.²³ We support this proposal. As the Report observes, “any new provision to clarify the ‘Australian link’ should be subject to careful consideration and further consultation to ensure that it does not have any unintended consequences — such as excluding an entity from the OAIC’s jurisdiction that Australians would expect to be covered.”²⁴

As the AGD considers such reforms, it is also important to avoid inadvertently capturing a range of entities that have little to no direct connection to Australia. For example, a data processor that is based outside Australia may still have an office in Australia — and it may use that office to process data about non-Australian individuals on behalf of its non-Australian business customers. It is not clear that the Act should apply in that scenario, because those activities do not involve the personal information of Australian individuals or the actions of Australian-based companies. Still, an overly broad interpretation of the “Australian link” could subject such processors to the Privacy Act, even though they may not be processing any personal information related to Australians. To avoid this result, BSA supports the Report’s suggestion that demonstrating an Australian link should include assessing not just whether the personal information is collected or held in Australia, but also whether the personal information is of an Australian or other individual physically located in Australia.²⁵

Recommendation: The AGD should conduct additional consultations to establish an “Australian link” sufficient to apply the Act to foreign organisations.

Mechanism to Prescribe Countries and Certification Schemes (Proposal 23.2)

The Report recommends introducing a mechanism to prescribe countries and certification schemes as providing “substantially similar protection” to the APPs under APP 8.2(a).²⁶ Importantly, the Report envisions that this new mechanism would be *one of several available methods* for companies to

²¹ Report (2023), p. 67.

²² Report (2023), p. 1.

²³ Report (2023), p. 236-237.

²⁴ Report (2023), p. 236.

²⁵ Report (2023), p. 236.

²⁶ Report (2023), p. 238.

transfer data internationally. This is critical because in order to achieve the goal of enhancing cross-border data transfers that create economic benefit to Australian businesses, the Act must clearly permit companies to transfer data internationally using a range of different transfer methods.

The Report recognises that companies can already transfer data to overseas recipients through a variety of methods consistent with the Act. These include disclosing data pursuant to APP 8.1, which adopts the accountability model and requires companies to meet certain obligations before transferring data to an overseas recipient. Separately, companies can also transfer data under APP 8.2 to an overseas recipient that is subject to a “substantially similar” privacy law or binding scheme, without adopting the obligations imposed in APP 8.1. Under the Report’s proposal, a mechanism would prescribe the countries and certification schemes that provide “substantially similar protection” under APP 8.2(a). The new mechanism would therefore make it easier for companies to transfer data under APP 8.2(a) by identifying countries that have “substantially similar protections,” rather than requiring companies to assess for themselves which countries have such protections. However, the new scheme would not limit companies from transferring data under the accountability model reflected in APP 8.1 or pursuant to any of the other grounds for transfers recognised in APP 8.2(b)-(f).

Regarding the proposal to recognise certification schemes that provide “substantially similar protection” to the Privacy Act, we recommend prescribing internationally recognised certification systems. This would support consumer confidence and improve business certainty. The Report notes that Australia could prescribe the APEC Cross Border Privacy Rules (**CBPR**) system under APP 8.2(a).²⁷ We support recognising the CBPR system as well as other internationally recognised certifications and standards that either exist today or that may be developed. For example, the Act could recognise compliance with ISO 27701 as creating “substantially similar” protections; that standard was published in 2019 and is the first data protection standard published by the International Standards Organization.

Recommendation: The AGD should conduct further consultations in creating a new mechanism to prescribe countries and certification schemes that provide “substantially similar” protections under APP 8.2(a).

As the AGD develops the new mechanism, it is also critical to set the appropriate conceptual metric for what constitutes a “substantially similar” level of privacy protection in order to facilitate responsible cross-border data transfers. If the mechanism establishes an unnecessarily strict interpretation of “substantially similar”, it would be counterproductive to the Report’s goal of increasing certainty for companies transferring data internationally. For example, to the extent a new mechanism applies the term “substantially similar” to mean a standard akin to the European Union’s “essentially equivalent” standard, it may unnecessarily restrict transfers conducted under APP 8.2(a).²⁸ Requiring foreign privacy laws deemed “substantially similar” to mirror, point-by-point, the APPs, would defeat the purpose of the mechanism. We recommend conducting further consultations on the process for, and factors involved in, determining whether a country or certification scheme offers the appropriate level of protection.

Standard Contractual Clauses (SCCs) (Proposal 23.3)

The Report proposes creating voluntary standard contractual clauses (**SCCs**) available to APP entities transferring information overseas.²⁹ Voluntary SCCs can be an important tool to reduce the burden on businesses to engage in contractual negotiations when transferring data across borders. SCCs also enable greater consistency in protecting data that is transferred out of Australia. At the same time, it is important to ensure any SCCs are voluntary, interoperable with existing SCCs recognised in other jurisdictions, and clearly satisfy the Act’s requirements.

²⁷ Report (2023), p. 247.

²⁸ We note that the GDPR’s adequacy determinations are based on the standard of “essential equivalence.” See: Questions & Answers on the adoption of the adequacy decision ensuring safe data flows between the EU and the Republic of Korea, December 2021, https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_6916.

²⁹ Report (2023), p. 239.

BSA agrees with the Report's observation that "SCCs should be designed in a way that is interoperable with the clauses developed by other jurisdictions to avoid organisations being required to enter into multiple SCCs."³⁰ Interoperable SCCs are more likely to be used by companies that operate across multiple jurisdictions, which further encourages the use of SCCs as a data transfer mechanism.

Recommendation: In developing SCCs, the AGD should ensure that any new SCCs: (1) are voluntary, (2) clearly satisfy the Act's transfer requirements (i.e., by supporting compliance with APP 8.1, or APP 8.2, or both), and (3) are interoperable with SCCs recognised in other jurisdictions.

Binding Corporate Rules

Binding corporate rules (**BCRs**) are used in several major jurisdictions to support international data transfers. In the European Union, for example, BCRs must be submitted by a company to the competent data protection authority for approval; the BCRs must ensure appropriate safeguards for data transfers and be legally binding and enforced by every party involved. The process for approving BCRs is recognised as rigorous, while providing a level of flexibility in facilitating transfers. Data protection laws in several other major jurisdictions, including Brazil, the United Kingdom, and Singapore, similarly support the use of BCRs for international data transfers.

Recommendation: The AGD should recognise that BCRs approved in other jurisdictions may support international data transfers under the Act. For example, this could be accomplished by recognising that BCRs approved in other jurisdictions provide substantially similar protection to the APPs, and therefore support transfers under APP 8.2(a). That approach would help to ensure both business certainty and efficiency while providing appropriate protections for personal data transfers.

Transfers Based on Informed Consent (Proposal 23.4)

In addition to transferring data under APP 8.1 (based on the accountability model) and APP 8.2(a) (based on "substantially similar" laws or binding schemes), the Act permits companies to transfer data for a range of other purposes, enumerated in APP 8.2(b)-(f). These include transferring data based on an individual's consent, pursuant to APP 8.2(b).

BSA supports retaining the informed consent exception in APP 8.2(b).³¹ We agree with the Report's findings that informed consent is "often relied on for data transfers," a "useful mechanism in circumstances where decisions and relationships are being managed at an individual level," and that "removing the exception would increase the regulatory burden for entities that rely on that exception." Moreover, it is important for the Act to provide a range of different methods for companies to transfer data internationally, with different safeguards that can account for the different contexts in which different types of data are transferred. Ensuring that individuals can consent to international transfers is important because it recognises that companies should be able to transfer data internationally at the request of an individual, even when other grounds for transfer are not available.

While the Report recommends retaining the informed consent exception, it also proposes adding a new requirement that disclosing entities consider the "risks" of an overseas disclosure and specifically inform individuals of any risks. Any such notification would be made in disclosures to consumers pursuant to APP 5. As noted below, those obligations should be more narrowly focused and better defined. For example, if a company discloses personal information to an overseas recipient that is subject to a law that provides substantially similar protections as the Act, it is not clear that any "risks" arise to justify notification. However, if a company relies on the informed consent exception to disclose that information to an overseas recipient, a notification may be appropriate.

Recommendation: The Act should retain the informed consent exception in APP 8.2(b), which recognises that an individual's consent is among one of several methods by which companies can transfer data internationally. Any new requirement to notify individuals of the "risks" of an overseas

³⁰ Report (2023), p. 239.

³¹ Report (2023), p. 240-241.

transfer should apply only when data is transferred under the informed consent exception — and not when data is transferred under other grounds recognised by the Act.

[Additional Notice Requirements for Transfers \(Proposal 23.5\)](#)

The Act already requires APP entities to notify individuals if they are likely to disclose an individual's personal information to an overseas recipient pursuant to APP 5.2(i). In addition, APP 5.2(j) also requires APP entities to notify individuals of the countries in which such recipients are likely to be located if it is practicable to do so. On top of these existing obligations, the Report recommends requiring APP entities to specify “the countries in which recipients are likely to be located if practicable . . . [and] the types of personal information that may be disclosed to recipients located overseas.”³²

Although improving transparency is important, these additional notices may lead to significantly longer disclosures to consumers that create more confusion without materially benefitting privacy. Indeed, the Report recognises that “including more granular detail in privacy policies would increase their complexity and the burden on customers to understand them and would require regular updates.”³³ Although the Report proposes shifting these disclosures from a generalized privacy policy to specific consumer disclosures made pursuant to APP 5.1(i), the concerns remain. Adding more information to an APP 5.1(i) disclosure may significantly lengthen the disclosures and draw attention away from other important information conveyed to the consumer, such as the purpose for which the information is collected.

Nor is it clear that additional disclosures improve consumers' privacy. The Report appears to assume that more granular disclosures would “allow individuals to make informed decisions about how their personal information is handled.” However, the Report's proposed additions to APP 5.1 are not clearly limited to disclosures made when seeking to transfer data overseas based on informed consent. Rather, the Report appears to recommend disclosures be required broadly, including in scenarios where the disclosures appear unnecessary, such as when personal information is transferred on grounds other than informed consent. For example, if an APP entity discloses personal information to an overseas recipient based on safeguards enacted pursuant to APP 8.1 or the entity discloses personal information to an overseas recipient subject to a “substantially similar law” under APP 8.2(a), the additional disclosures envisioned by the Report may do little to increase the substantive privacy protections for that information.

Recommendation: The Act should not require APP entities to notify individuals under APP 5.1 of the types of personal information that may be disclosed overseas. To the extent any such requirement is imposed, it should apply only to disclosures made when seeking consent to transfer data pursuant to the informed consent exception.³⁴

[Direct Right of Action and Statutory Tort for Invasion of Privacy \(Proposals 26 and 27\)](#)

The Report recommends several changes to the Act's enforcement, including: (1) creating a direct right of action for individuals,³⁵ and (2) introducing a statutory tort for serious invasions of privacy.³⁶

BSA does not support these recommendations. Although privacy laws should be subject to robust and effective enforcement, that enforcement should be led by agencies, which can create a consistent body of enforcement actions that demonstrate how they will apply privacy rights and obligations in a variety of contexts, particularly when combined with informal or formal guidance interpreting the privacy law. A consistent, agency-led approach provides much-needed clarity for consumers and

³² Report (2023), p. 241-242.

³³ Report (2023), p. 241.

³⁴ Report (2023), p. 241.

³⁵ Report (2023), p. 279.

³⁶ Report (2023), p. 287.

entities as to how the rights and obligations under the Act will apply. 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. Although the Report suggests this would “benefit individuals and APP entities by clarifying the application of the Act,”³⁷ in practice it is likely to result in differing decisions by different courts that can create confusion for both consumers and companies about how the Act is to apply. This will create a less certain enforcement environment for companies and less useful guidance to individuals and entities wanting to understand their rights and obligations in advance.

Further, if both direct rights of action and a statutory tort for invasion of privacy are introduced, potential litigants may bring multiple claims for a single activity, potentially resulting in resource-wasteful litigation while offering the litigants two opportunities to sue for the same alleged violation.

The experience of the implementation of the CCPA is illustrative of the 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 businesses, as individuals or a class, 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.³⁸ 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 the fact 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.³⁹ 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.

Recommendation: The Act should *not* include a direct right of action and statutory tort. Instead, enforcement should remain agency led to impose consistency and predictability to both businesses and consumers. If a direct right of action is introduced, the participation of the enforcing agency in the court proceedings should be made mandatory to enhance regulatory coherence.

The “Fair and Reasonable Test” (Proposals 12.1–12.3)

The Report proposes adopting a “fair and reasonable” test under which APP entities would determine if handling of individuals’ personal information is permissible under the Act.⁴⁰ While the Report recognises this test creates a large degree of uncertainty, it proposes reducing that uncertainty in part by identifying in the Act a list of factors that entities may consider in determining if an activity is fair and reasonable.

Although we appreciate that the proposal for a “fair and reasonable” test draws from current APP obligations, including APPs 3 and 6, the application of this test will necessarily involve a large degree of uncertainty even with statutory factors that help guide companies. This test — and the corresponding legislative factors — must be flexible in order to apply to the wide range of activities covered by the Act. Given that flexibility, such a test is best suited to enforcement by a central regulator that can issue guidance about how the standard is to apply over time and in different scenarios, to promote consistent outcomes that appropriately reflect trade-offs that are likely to be involved in applying legislative factors in different scenarios. We recommend that the AGD prioritise the need for consistent enforcement of any “fair and reasonable” test, particularly in light of the

³⁷ Report (2023), p. 273.

³⁸ 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>.

³⁹ 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>.

⁴⁰ Report (2023), p. 116.

Report's separate proposal to create a direct right of action.⁴¹ To the extent a new "fair and reasonable" test is enforced through private litigation, it may lead to the test being applied inconsistently, even when cases involve similar types of processing.

Recommendation: If a "fair and reasonable" test is introduced, it should be enforced solely via the enforcement agency, to create consistent regulatory enforcement of this obligation, which can better protect consumer privacy and create greater certainty for APP entities.

Legitimate Interests

The Report does not propose recognising legitimate interests as a lawful basis for processing personal information in Australia. The Report expresses concerns that adopting lawful bases for processing would "fundamentally change the current principles-based approach in the Act" and that APPs 3 and 6 already provide a flexible framework that allows for the collection, use, and disclosure of personal information for the purposes set out in the GDPR's lawful bases.⁴² The Report also suggests that adopting bases for processing could require adopting the concept of "processing" and questions whether the approach would result in "a more privacy protective outcome for Australians."⁴³

As the AGD further considers these issues, we recommend reconsidering the potential for incorporating a legitimate interest basis for processing into the Act. At the outset, it is not apparent that introducing a legitimate interests basis for processing would lead to a "fundamental change" in the principles-based approach in the Act. The APPs, which currently focus on consent as a lawful basis for handling personal information, could be amended to recognise legitimate interests. Furthermore, this change could be paired with the implementation of a fair and reasonable test across the Act, which already requires certain fundamental changes to the Act and can provide guardrails for ensuring that personal information is processed lawfully, fairly, and in a transparent manner that creates effective consumer protections.⁴⁴

Introducing a legitimate interest basis can result in better privacy outcomes for Australians. As acknowledged by the Report, consent should be reserved for situations where it is most meaningful to consumers, such as "high privacy risk situations."⁴⁵ By recognising additional bases for processing personal information in addition to consent, privacy laws can further reduce the unnecessary burden on consumers to provide consent to each expected use of their personal information. 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. The legitimate interests basis would provide companies appropriate flexibility to process personal information for these purposes.

Recommendation: BSA supports recognising legitimate interests as a lawful basis for the processing of personal information and encourages the AGD to include legitimate interests as a complement to the recommendation to adopt a "fair and reasonable" test.

Artificial Intelligence (AI) and Automated Decision-Making (ADM) (Proposals 19.1–19.3)

The Report proposes several new obligations related to automated decisions that have "legal or similarly significant effect" on an individual's rights. These include: (1) requiring privacy policies to set out the types of personal information that will be used in substantially automated decisions that have such effects; (2) requiring the Act to include high-level indicators of the types of decisions that have "legal or similarly significant effects" and require OAIC to supplement that legislative text with

⁴¹ Report (2023), Proposal 26.

⁴² Report (2023), p. 113.

⁴³ Report (2023), p. 113.

⁴⁴ Introducing the concept of "processing" does not appear to be a significant hurdle to adopting a legitimate interests ground for processing because introducing the concept of "processing" may already be necessary to introduce a controller-processor distinction.

⁴⁵ Report (2023), p. 103.

guidance; and (3) introducing a new right for individuals to request “meaningful information about how substantially automated decisions with legal or similarly significant effect are made.” We appreciate the Report’s suggestion that these proposals should be coordinated with any broader work undertaken on AI and ADM, including ongoing consultations with other agencies.

In defining decisions with “legal or similarly significant effects,” we encourage the AGD to create a comprehensive definition to increase certainty for both individuals and companies about when related rights are available. For example, the Act could define these terms in a manner similar to state privacy laws in the United States, where Virginia, Colorado, and Connecticut all create rights to opt out of certain types of profiling that create legal or similarly significant effects.⁴⁶ Creating obligations and rights that are interoperable with other privacy laws also ensures that individuals and companies are better able to apply these protections across jurisdictions and drives investment by businesses in effective compliance programs.

In addition, any new individual rights related to automated processing should be exercised in a manner similar to other new individual rights: by individuals exercising those rights through a controller rather than via a processor acting on behalf of a controller.

More broadly, as it considers AI-related issues, we urge the AGD to ensure any AI provisions recognise the variety of stakeholders that may play a role in designing and using an AI system. In general, there are at least two key stakeholders with varying degrees of responsibility for managing the risks associated with an AI system throughout its lifecycle. First, an AI *developer* is an organisation responsible for the design and development of an AI system. Second, an AI *deployer* is an organisation that uses an AI system.⁴⁷ By recognising the different roles of developers and deployers, policymakers can tailor obligations to an organisation’s role in the AI marketplace. For example, a deployer using an AI system does not generally have control over design decisions made by another company that developed the AI system. Likewise, a developer of an AI system generally does not have control over subsequent uses of the AI system by another company deploying the system.⁴⁸ We encourage the AGD to bear these roles in mind as it further considers AI-related issues.

Recommendation: The Act should clearly define “legal or similarly significant effects” and ensure any new individual rights relating to automated decision-making are interoperable with rights created in other privacy laws internationally. More broadly, the AGD should ensure any provisions affecting AI systems reflect the different roles that different companies play in creating and using those systems, including the distinct roles of developers and deployers.

“Serious” Interference with Privacy (Proposal 25.2)

The Report proposes amending section 13G of the Act, which creates penalties for “serious and repeated interferences with privacy.” The proposal would remove the word “repeated” from the Act

⁴⁶ See Colorado Privacy Act, Sec. 6-1-1303(10) (“Decisions that produce legal or similarly significant effects concerning a consumer” is defined as “a decision that results in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services, or access to essential goods or services.”); Connecticut Data Privacy Act Sec.1(22) (“Decisions that produce legal or similarly significant effects concerning the consumer” are defined as “decisions made by the controller that result in the provision or denial by the controller of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services or access to essential goods or services.”); Virginia Consumer Data Protection Act, Sec. 59.1-575 (“Decisions that produce legal or similarly significant effects concerning a consumer” are defined as “a decision made by the controller that results in the provision or denial by the controller of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities, such as food and water.”).

⁴⁷ AI Developers and Deployers: An Important Distinction, March 2023, <https://www.bsa.org/policy-filings/ai-developers-and-deployers-an-important-distinction>.

⁴⁸ The importance of such an approach to AI regulation is a key pillar of the Organisation for Economic Co-operation and Development’s (OECD’s) Recommendation of the Council on Artificial Intelligence, which recognises that effective AI policies must account for “stakeholders according to their role and the context” in which AI is being deployed. See Recommendation of the Council on Artificial Intelligence, May 2019, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>. Per the Recommendation, the AI stakeholder community “encompasses all organizations and individuals involved in, or affected by, AI systems, directly or indirectly.

and create a list of actions that may amounts to a “serious” interference with privacy. This legislative text would be supplemented by further guidance from the OAIC.⁴⁹

BSA supports this proposal as it will provide businesses with greater clarity about conduct that can trigger Section 13G’s penalties. This is particularly important given the recent increase in maximum civil penalties under Section 13G. We appreciate the importance of listing actions that may fall within Section 13G, such as breaches involving sensitive information, actions adversely affecting large groups of individuals or impacting vulnerable individuals, repeated or wilful misconduct, and serious failures to take proper steps to protect personal data. Identifying actions that may be significant can create a shared understanding between regulators and businesses about the violations that may trigger such penalties. At the same time, we urge the AGD to create further specificity around some of the factors identified in the Report. For example, it is possible that any violation by a large company that serves many business and individual consumers could “adversely affect large groups of individuals” simply because of the volume of consumers that use its services. Factors applying Section 13G should not automatically treat such a violation as significant but be applied in a risk-based manner that avoids treating a single factor as determinative.

In addition to listing factors in 13G to identify “serious” violations, the Act or implementing guidance should also identify mitigating factors to be considered in determining any penalty under this section. For example, prompt reporting of a violation or breach and cooperation with the relevant authorities may appropriately be considered a mitigating factor. Identifying such mitigating factors can encourage businesses to adopt a “honesty is the best policy” approach, which can facilitate investigations.

Recommendation: The AGD should revise Section 13G to not only define actions that may constitute a “serious” interference with privacy, but also to identify mitigating actions relevant to penalties under Section 13G.

Additional Recommendations: Scope and Application of the Privacy Act

Small Business Exemption (Proposals 6.1–6.2)

The Report proposes removing the small business exception after taking certain steps to understand the impact of removing the exception and after consulting with small businesses. As the Report observes, the small business exemption “may no longer be acceptable to the community when considered in the context of technology proliferation and increased use of personal information for online sales and marketing, background analytics and data-related partnerships.”⁵⁰

While BSA acknowledges the need for further consultations, the AGD should establish a clear timeline for consultations and set a date for sunseting the exemption to provide certainty and enable businesses to plan accordingly.

Recommendation: The AGD should remove the small business exemption from the Act and should prescribe clear timelines on consultations about its removal and set a date for sunseting the exemption.

Definition of Personal Information (Proposals 4.1–4.2)

The Report proposes several changes to the definition of personal information covered by the Act. These include defining personal information as information that “relates to” an individual rather than information “about” an individual. BSA agrees with the Report’s observation that “there needs to be a relationship between the information and the individual,”⁵¹ lest the definition become too broad.⁵² In addition, the Report proposes including a non-exhaustive list of information that may be personal

⁴⁹ Report (2023), p. 258.

⁵⁰ Report (2023), p. 56.

⁵¹ Report (2023), p. 25.

⁵² Report (2023), p. 27.

information to help APP entities identify information covered by the Act. BSA supports this proposal, which can give entities more certainty about their obligations.

Recommendation: BSA supports proposals to: (1) ensure that the definition of “personal information” is confined to where the connection between the information and individual is not too tenuous or remote, and (2) include a non-exhaustive list of examples of personal information to assist APP entities. We encourage the AGD and the OAIC to work closely with the private sector through consultations and working groups to draft guidance materials.

Definition of “De-identified” (Proposals 4.5-4.6)

The Report proposes to amend the definition of “de-identified” to make it clear that de-identification is a process, informed by best available practice, applied to personal information which involves treating it in such a way such that no individual is identified or reasonably identifiable in the current context. The Report also proposes to extend specific APPs to de-identified information.

The Report’s approach creates significant confusion about what will be deemed “de-identified” under the Act. To the extent “de-identified” means “anonymised”, such data should *not* be subject to the Act. If “de-identified” means “pseudonymised”, then applying a targeted subset of APPs to that information may be appropriate and encourage companies to process data in de-identified form rather than in a personally identifiable format.

Recommendation: The Act should clearly define “de-identified” information. To the extent de-identified information is addressed by the Act, it should be subject only to a subset of APP protections.

Additional Recommendations: Protections

Consent (Proposal 11.1)

The Report proposes amending the definition of consent to provide that it must be voluntary, informed, current, specific, and unambiguous. We agree with the Report that, while consent is an important mechanism for the collection, use, and disclosure of personal information, it is “most effective when used in a narrow range of situations where individuals most need to exert control over their personal information.”⁵³ Consent should be reserved for situations where it is most meaningful to consumers, such as “high privacy risk situations” as proposed by the OAIC,⁵⁴ to avoid burdening consumers with a high volume of consent requests that increases consent fatigue. We support the proposal to amend the definition of consent to provide that it must be “voluntary, informed, current, specific, and unambiguous,” which is more specific and will provide businesses with a clearer idea of what would constitute consent. However, the Act should *not* be amended to increase the circumstances in which consent is required.

Recommendation: The Act should define consent to provide that it must be “voluntary, informed, current, specific, and unambiguous.” The OAIC should also supplement this definition with guidance on its application, in consultation with stakeholders including the private sector.

Individual Rights Requests (Proposals 18.1–18.3)

The Report recommends providing important individual rights, including access and correction. As these rights are implemented, it is crucial to clearly state in the Act that controllers, and not processors, should be the recipients of, and responsible for responding to, requests regarding consumer privacy rights. In this regard, while the Report acknowledges that the controller-processor distinction would “assist with clarifying obligations in relation to any new individual rights (such as a right to erasure) that may be introduced following this Review,”⁵⁵ it did not specifically focus on the need for individuals to exercise these rights by submitting their requests or queries to a controller.

⁵³ Report (2023), p. 102.

⁵⁴ Report (2023), p. 103.

⁵⁵ Report (2023), p. 231.

BSA also agrees with the Report that these individual rights are generally not absolute and, as such, supports the proposed imposition of appropriate exceptions to individual rights requests.⁵⁶

Recommendation: The Act should clearly state that controllers, and not processors, are the appropriate recipients of, and responsible for responding to, individual rights requests. BSA also supports imposing appropriate exceptions to individual rights requests.

Direct Marketing and Targeted Advertising (Proposals 20.2–20.3)

The Report proposes amending the Act to create new rights for individuals to opt out of their personal information being used or disclosed for direct marketing or targeted advertising.

In implementing these new rights, we encourage the AGD to ensure that individuals exercise their rights to opt-out of direct marketing and targeted advertising by submitting such requests directly to controllers, rather than to processors acting on behalf of controllers. This approach is in line with many data protection and privacy laws internationally, which recognise that processors should not be subject to consumer-facing obligations, including rights to opt out of targeted advertising.

Recommendation: Individuals should exercise new rights to opt-out of direct marketing and targeted advertising by submitting their requests to data controllers, which are the entities positioned to honour such requests.

Security, Retention, and Destruction (Proposals 21.1, 21.3, and 21.5)

The Report proposes amending several aspects of APP 11, which creates important data security obligations. BSA agrees with the Report's observations that "[i]ndustry would benefit from further guidance and education outlining the Government's cyber security expectations under the Act, particularly as the threat environment changes over time."⁵⁷ Guidance on reasonable steps that businesses can take to secure, destroy, and de-identify personal information will better help companies meet their obligations and more effectively allocate resources. For example, in creating guidance on reasonable steps that businesses can take to secure data, the OAIC could encourage organisations to move toward zero trust architecture and security measures, including multi-factor authentication. Providing examples of specific reasonable steps that businesses can adopt would improve business certainty regarding compliance with information security related obligations.

Recommendation: The OAIC should provide clear guidance on what "reasonable steps" are required to comply with APP 11, including through materials on reasonable steps to secure, destroy, and de-identify personal information. This may include providing specific examples of reasonable cybersecurity practices to that can help businesses secure their data.

Temporary APP Codes and Emergency Declarations (Proposal 5.2 and 5.4)

The Report states that the current process for developing APP codes "can be lengthy."⁵⁸ Proposal 5.2 suggests amending the Act to create new powers for the Commissioner to issue temporary APP Codes.⁵⁹ Notably, this process of code development would not require some of the regular and valuable processes normally involved in creating Codes, including consultation with relevant stakeholders. The Report illustrates the need for this proposed change by citing the recent global pandemic.

Proposal 5.4 recommends extending the application of Emergency Declarations to apply to ongoing emergencies and again cites the pandemic as an example of why the amendment is needed.⁶⁰

⁵⁶ Report (2023), Proposal 18.6.

⁵⁷ Report (2023), p. 224.

⁵⁸ Report (2023), p. 49.

⁵⁹ Report (2023), p.50.

⁶⁰ Report (2023), p. 51.

While Proposal 5.4 seems reasonable in the scenario used to illustrate the application of this power, it also makes Proposal 5.2 somewhat redundant. In this context it seems to be a considerable power with no considerable need.

Recommendation: If Proposal 5.4 is enacted, the AGD should not implement Proposal 5.2. The AGD should also provide clear guidance to industry on the types of scenarios that would trigger implementing emergency powers.

Standardised Templates (Proposal 10.3)

The Report proposes that standardised templates and layouts for privacy policies and collection notices, as well as standardised terminology and icons, should be developed by reference to relevant sectors while seeking to maintain a degree of consistency across the economy.⁶¹

The Report also notes that it is impractical to develop one standardised template, lexicon, or icon for use across all APP entities because of the wide range of contexts in which the Act applies. Templates might be helpful for smaller businesses or businesses engaging with the APPs for the first time. However, it is important that any such materials be voluntary, so that businesses may appropriately tailor their information to customers based on their particular products and services.

Recommendation: The AGD should ensure any standardisation of privacy policies or collection notices is voluntary while allowing business to continue to meet appropriate standards through a principles-based approach.

Conclusion

We thank the AGD for the opportunity to submit comments on the Report and appreciate the AGD's consideration of our recommendations. We hope that our concerns and recommendations will assist in the development of a rigorous and effective privacy regime, which enhances privacy protections while providing regulatory certainty for businesses. We would be happy to meet with the AGD to discuss our submission and appreciate 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

⁶¹ Report (2023), p. 99-100.



Controllers and Processors: A Longstanding Distinction in Privacy

Modern privacy laws have coalesced around core principles that underpin early privacy frameworks. For example, leading data protection laws globally incorporate principles of notice, access, and correction. They also identify appropriate obligations for organizations in fulfilling these rights, making important distinctions between companies that decide how and why to process personal data, which act as controllers of that data, and companies that process the data on behalf of others, which act as processors of such data. Privacy and data protection laws worldwide also assign different obligations to these different types of entities, reflecting their different roles in handling consumers' personal data.

The concepts of controllers and processors have existed for more than forty years. These roles are key parts of global privacy and data protection frameworks including the OECD Privacy Guidelines, Convention 108, the APEC Privacy Framework, and ISO 27701.

The History of Controllers and Processors

1980: OECD PRIVACY GUIDELINES

The OECD Privacy Guidelines launched the modern wave of privacy laws, building on earlier efforts including a 1973 report by the US Department of Health, Education and Welfare that examined privacy challenges posed by computerized data processing and recommended a set of fair information practice principles.¹

The OECD Guidelines, adopted in 1980, define a "**data controller**" as the entity "competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf."²

Comments to the 1980 Guidelines recognize "[t]he term 'data controller' is of vital importance" because it defines the entity "legally competent to decide about the contents and use of data."³

1981: COUNCIL OF EUROPE CONVENTION 108

The Council of Europe in 1981 opened for signature the first legally binding international instrument in the data protection field. Convention 108 defined a "**controller of the file**" as the person "competent . . . to decide" the purpose of automated files, as well as "which categories of personal data should be stored and which operations should be applied to them."⁴

1995: EU DATA PROTECTION DIRECTIVE

The 1995 EU Data Protection Directive, which previously formed the basis of privacy laws in EU member countries, separately defined both controllers and processors.⁵ **Controllers** were defined as the natural or legal person that "determines the purposes and means of the processing of personal data," while **processors** were defined as a natural or legal person "which processes personal data on behalf of the controller."

2005: APEC PRIVACY FRAMEWORK

The APEC Privacy Framework builds on the OECD Privacy Guidelines and provides guidance on protecting privacy, security, and the flow of data for economies in the APEC region. It was endorsed by APEC in 2005 and updated in 2015. The Framework defines a **controller** as an organization that “controls the collection, holding, processing, use, disclosure, or transfer of personal information,” including those instructing others to handle data on their behalf. It does not apply to entities processing data as instructed by another organization.⁶

2011: APEC CROSS-BORDER PRIVACY RULES (CBPR) SYSTEM

All 21 APEC economies endorsed the Cross-Border Privacy Rules (CBPR) System in 2011, creating a government-backed voluntary system designed to implement the APEC Privacy Framework.⁷ The CBPR system is limited to **data controllers**. In 2015, APEC created a separate Privacy Recognition for Processors (“PRP”) System to help controllers identify qualified and accountable **processors**.⁸

2016: EU GENERAL DATA PROTECTION REGULATION

The EU General Data Protection Regulation replaced the 1995 Directive, maintaining the definition of **controller** as the entity that “determines the purposes and means” of processing personal data, and the definition of **processor** as the entity that “processes personal data on behalf of the controller.”⁹ It was adopted in 2016 and took effect in 2018.

2018: COUNCIL OF EUROPE MODERNIZED CONVENTION 108

Convention 108 was modernized in 2018, revising the definition of **controller** and adding a definition of processor. A controller is the entity with “decision-making power with respect to data processing.”¹⁰ A **processor** “processes personal data on behalf of the controller.”¹¹

2019: ISO 27701

The International Organization for Standardization published ISO 27701 in 2019, creating the first international standard for privacy information management. ISO 27701 allocates obligations to implement privacy controls based on whether organizations are controllers or processors. It recognizes that a **controller** determines “the purposes and means of processing”¹² while **processors** should ensure that personal data processed on behalf of a customer is “only processed for the purposes expressed in the documented instructions of the customer.”¹³

2023: US STATE PRIVACY LAWS




In the United States, five new state consumer privacy laws will take effect in 2023, in California, Colorado, Connecticut, Utah, and Virginia. All five laws distinguish between **controllers** or businesses that determine the purpose and means of processing, and **processors** or service providers that handle personal information on behalf of the controller or business.






According to a March 2021 report, **more than 84%** of countries responding to an OECD questionnaire define “data controller” in their privacy legislation.¹⁴

Controllers and Processors: A Distinction Adopted Around the World

Privacy laws worldwide draw from longstanding privacy frameworks, recognizing the distinction between controllers and processors and assigning different responsibilities to these different entities based on their different roles in processing personal data. The chart below identifies some of the countries with national privacy or data protection laws that reflect the roles of controllers and processors.

 JURISDICTION	 CONTROLLER	 PROCESSOR
Brazil ¹⁵	Controller: A “natural person or legal entity . . . in charge of making the decisions regarding the processing of personal data.”	Processor: A “natural person or legal entity . . . that processes personal data in the name of the controller.”
Cayman Islands ¹⁶	Data Controller: A “person who, alone or jointly with others <i>determines the purposes, conditions and manner</i> in which any personal data are, or are to be, processed”	Data Processor: Any person “who processes personal data <i>on behalf of</i> a data controller but, for the avoidance of doubt, does not include an employee of the data controller.”
European Union ¹⁷	Controller: A natural or legal person that “alone, or jointly with others, <i>determines the purposes and means of processing</i> personal data”	Processor: A natural or legal person that “processes personal data <i>on behalf of</i> the controller.”
Faroe Islands ¹⁸	Controller: A natural or legal person that “alone or jointly with others, <i>determines the purposes and means of the processing of</i> personal data.”	Processor: A natural or legal person that “processes personal data <i>on behalf of</i> the controller.”
Hong Kong ¹⁹	Data User: A person who “either alone or jointly or in common with other persons, <i>controls the collection, holding, processing or use of the data.</i> ”	Data Processor: A “person who: (a) Processes personal data <i>on behalf of</i> another person; and (b) <i>Does not process the data for any of the person’s own purposes.</i> ”
Kosovo ²⁰	Data Controller: A natural or legal person that “alone or jointly with others, <i>determines purposes and means of personal data processing.</i> ”	Data Processor: A natural or legal person that “processes personal data for and <i>on behalf of</i> the data controller.”
Malaysia ²¹	Data User: A person “who either alone or jointly or in common with other persons processes any personal data or <i>has control over or authorizes</i> the processing of any personal data, but <i>does not include a data processor.</i> ”	Data Processor: A person “who processes the personal data solely <i>on behalf of</i> the data user, and <i>does not process the personal data for any of his own purposes.</i> ”
Mexico ²²	Data Controller: An individual or private legal entity “ <i>that decides on the processing of</i> personal data.”	Data Processor: The individual or legal entity that “alone or jointly with others, processes personal data <i>on behalf of</i> the data controller.”
Philippines ²³	Personal Information Controller: A person or organization “ <i>who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf. The term excludes a person or organization who performs such functions as instructed by another person or organization.</i> ”	Personal Information Processor: A natural or juridical person “to whom a personal information controller may <i>outsource</i> the processing of personal data pertaining to a data subject.”
Qatar ²⁴	Controller: A natural or legal person “who, whether acting individually or jointly with others, <i>determines how Personal Data may be processed and determines the purpose(s) of any such processing.</i>”	Processor: A natural or legal person “who processes Personal Data for the Controller.”
Singapore ²⁵	Organisation: Any individual, company, association or body of persons, corporate or unincorporated, whether or not: (a) formed or recognized under the law of Singapore or (b) resident, or having an office or a place of business, in Singapore.	Data Intermediary: An organisation “which processes personal data <i>on behalf of another organisation</i> but does not include an employee of that other organisation.”

 JURISDICTION	 CONTROLLER	 PROCESSOR
South Africa ²⁶	Responsible Party: A public or private body or any other person that “alone or in conjunction with others, determines the purpose of and means for processing personal information.”	Operator: A person who “processes personal information for a responsible party in terms of a contract or mandate, without coming under direct authority of that party.”
Thailand ²⁷	Data Controller: A person or juristic person “having the power and duties to make decisions regarding the collection, use, or disclosure of the Personal Data.”	Data Processor: A person or juristic person who “operates in relation to the collection, use, or disclosure of Personal Data pursuant to the orders given by or on behalf of the Data Controller.”
Turkey ²⁸	Data Controller: A natural or legal person “who determines the purposes and means of processing personal data.”	Data Processor: A natural or legal person “who processes personal data on behalf of the data controller upon its authorization.”
Ukraine ²⁹	Personal Data Owner: A natural or legal person who “determines the purpose of personal data processing, the composition of this data and the procedures for its processing.”	Personal Data Manager: A natural or legal person who is “granted the right by the personal data owner or by law to process this data on behalf of the owner.”
United Kingdom ³⁰	Controller: A natural or legal person that “alone or jointly with others, determines the purposes and means of the processing of personal data.”	Processor: A natural or legal person that “processes personal data on behalf of the controller.”

Endnotes

- Dept. of Health, Educ., & Welfare, Records, Computers, and the Rights of Citizens (1973), <https://aspe.hhs.gov/reports/records-computers-rights-citizens>.
- OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, § 1(a) (1980), <https://www.oecd.org/sti/ieconomy/oecdguidelinesonthe protectionofprivacyandtransborderflowsofpersonaldata.htm>.
- Id.* at Explanatory Memorandum, § IIB, para. 40.
- Council of Europe, Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data, art. 2(d), Jan. 28, 1981, ETS No. 108, <https://rm.coe.int/1680078b37>.
- Directive 95/46/EC, art. 2(d)-(e), <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX%3A31995L0046%3AEN%3AHTML>.
- APEC, APEC Privacy Framework (2015), § II.10, <https://cbprs.blob.core.windows.net/files/2015%20APEC%20Privacy%20Framework.pdf>.
- See APEC, 2011 Leaders' Declaration, https://www.apec.org/meeting-papers/leaders-declarations/2011/2011_aelm; <http://cbprs.org/privacy-in-apec-region/>.
- See APEC Privacy Recognition for Processors (“PRP”) Purpose and Background, <https://cbprs.blob.core.windows.net/files/PRP%20-%20Purpose%20and%20Background.pdf>.
- EU General Data Protection Regulation, art. 4(7)-(8), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>.
- Council of Europe, Modernised Convention for the Protection of Individuals With Regard to the Processing of Personal Data, art. 2(d), May 17-18, 2018, ETS No. 108, https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf.
- Id.* at art. 2(f).
- Int'l Org. for Standardization, International Standard ISO/IEC 27701 Security Techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management—Requirements and Guidelines 1, 4-5, 29-55 (2019).
- Id.* at 43.
- OECD, Report on the Recommendation of the Council Concerning Guidelines Governing Protection of Privacy and Transborder Flows of Personal Data, 16 (2021), <https://www.oecd.org/sti/ieconomy/privacy.htm>.
- Law No. 13,709, Aug. 14, 2018, art. 5 VI-VII (as amended by Law No. 13,853, July 8, 2019, Official Journal of the Union [D.O.U.] July 9, 2019), https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf.
- Data Protection Act (2021), § 2, https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf.
- EU General Data Protection Regulation, art. 4, 2016 O.J. (L 119), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3A%3A2016%3A119%3ATOC>.
- Act on the Protection of Personal Data No. 80 (2020), §§ 6(6)-(7), <https://dat.cdn.f0/media/opcxh1q/act-on-the-protection-of-personal-data-data-protection-act-act-no-80-on-the-7-june-2020.pdf?s=LA6lqXBchs1Ryn1Kp9h3KSPuFog>.
- Personal Data (Privacy) Ordinance, (1996) Cap. 486, § 2(1), <https://www.elegislation.gov.hk/hk/cap486>. See https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html.
- Law No. 06/L-082 on Protection of Personal Data (2019), art. 3, §§ 1.11, 1.14, https://www.dataguidance.com/sites/default/files/law_no_06_l-082_on_protection_of_personal_data_0.pdf.
- Act 709 Personal Data Protection Act 2010, § 4, <https://ilo.org/dyn/natlex/docs/ELECTRONIC/89542/102901/F1991107148/MYS89542%202016.pdf>.
- Federal Law on Protection of Personal Data Held by Private Parties, art. 3, XIV & IX, Official Gazette July 5, 2010, <https://www.dataguidance.com/legal-research/federal-law-protection-personal-data-held>.
- Data Privacy Act of 2012, Rep. Act No. 10173, §§ 3(h)-(i) (Aug. 15, 2012), <https://www.officialgazette.gov.ph/2012/08/15/republic-act-no-10173/#:~:text=11.,transparency%2C%20legitimate%20purpose%20and%20proportionality>.
- Law No. 13 of 2016 Personal Data Privacy Protection, art. 1, https://www.dataguidance.com/sites/default/files/law_no_13_of_2016_on_protecting_personal_data_privacy_-_english.pdf.
- Personal Data Protection Act 2012, as amended, § 2(1), <https://sso.agc.gov.sg/Act/PDPA2012>.
- Protection of Personal Information Act, 2013, Act 4 of 2013, Chap. 1, <https://popia.co.za/>.
- Personal Data Protection Act, B.E. 2562 (2019), § 6, <https://cyrilla.org/es/entity/si9175g71u?page=1>.
- Law on Protection of Personal Data No. 6698 (2016), art. 3(g), 3(i), <https://www.kvkk.gov.tr/icerik/6649/Personal-Data-Protection-Law>.
- Law of Ukraine on Personal Data Protection (2010) (as amended), art. 2, 4(4), <https://zakon.rada.gov.ua/laws/show/en/2297-17#Text>.
- UK General Data Protection Regulation 2016 (as amended), c. 1, art. 4(7)-(8), <https://www.legislation.gov.uk/eur/2016/679>. See also UK Information Commissioner's Office, Who Does the UK GDPR Apply To?, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/>.