Comments to the Attorney-General's Department of the Government of Australia on the Review of the Privacy Act 1988

The Global Data Alliance[1] welcomes the opportunity to share its views on the review of the Australian Privacy Act 1988 (the **Act**), which the Attorney-General's Department published on October 30, 2020.[2] Various aspects of the current Review are very important to Global Data Alliance members, and comments on those issues are being communicated to you through different submissions, and we ask that you consider them. This letter respectfully presents our specific views regarding cross-border data flows, as this is the focus of the Global Data Alliance.

The Alliance is a cross-industry coalition of companies, headquartered in different regions of the world, that are committed to high standards of data privacy and security. Alliance companies rely on the ability to transfer data responsibly around the world to create jobs and make local industries more competitive. Cross-border data transfers power innovation and growth across the globe and all sectors of the economy — from manufacturing and farming to local start-ups and service providers. Data transfers enable the digital tools and insights that are critical to enabling entrepreneurs and companies of all sizes, in every country, to create new kinds of jobs, boost efficiency, drive quality, and improve output[3].

Global Data Alliance members share a deep and long-standing commitment to protecting personal data across technologies and business models, as they recognize that today's cross-border economy depends on the trust of consumers and the general public. The Alliance, therefore, supports policies that protect personal data while enabling data to move across borders.

We are hopeful that the amended Privacy Act that will result from this Review will promote robust personal information protection through a legal framework that is flexible, fosters innovation, and allow companies to responsibly transfer data both internally and externally to other entities, within and outside Australia.

The seamless transfer of data across international borders is critical to cloud computing, data analytics, global fraud monitoring and prevention, and other modern and emerging technologies and services that underpin the global economy and benefit all sectors of the economy. Furthermore, a forward-leaning policy on cross-border data transfers, which is interoperable with international frameworks, is a particularly effective tool to aid policymaker efforts to drive innovation, increase employment, and create other economic and societal benefits for government, businesses, consumers, and society.

---

[1] The Global Data Alliance is a cross-industry coalition of companies that are committed to high standards of data responsibility and that rely on the ability to transfer data around the world to innovate and create jobs. The Alliance supports policies that help instill trust in the digital economy while safeguarding the ability to transfer data across borders and refraining from imposing data localization requirements that restrict trade. Alliance members include BSA members and American Express, Amgen, AT&T, Citi, ITB360, LEGO, Mastercard, Medtronic, Panasonic, Pfizer, Roche, United Airlines, Verizon, Visa, UDS Technology, and WD-40 Company. BSA | The Software Alliance administers the Global Data Alliance. For more information on the Global Data Alliance, please see: https://www.globaldataalliance.org/downloads/aboutgda.pdf

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

[3] Please see Global Data Alliance paper "The Cross-Border Movement of Data: Creating Jobs and Trust Across Borders in Every Sector available at https://www.globaldataalliance.org/downloads/GDAeverysector.pdf.

Accountability Model and International Data Transfers

The GDA strongly supports the accountability model for international data transfers. This model was, first established by the OECD and subsequently endorsed and integrated in many legal systems and privacy principles, including the Act and Australia Privacy Principles (**APPs**). The accountability model provides an approach to cross-border data governance that effectively protects the individual and fosters streamlined, robust data flows by requiring entities that collect personal information (often defined as data controllers) to be responsible for its protection, no matter where or by whom it is processed.

The notion that data privacy and security are negatively impacted by the ability to transfer data across borders is mistaken. Proposals that claim or suggest that data can either flow across borders or remain secure by being stored locally present a false choice, and closing digital borders will not help achieve data privacy and security objectives. The Review cites the example of how the Privacy Act was amended to implement privacy protections for information collected by the COVIDSafe App where specific provisions were introduced to ensure data was stored within Australia and to prohibit the overseas transfer of COVID app data.[4] While governments are rightfully concerned with privacy risks and data security, these concerns are ultimately not dependent on the physical location of the data, or the location of the infrastructure supporting it, particularly given the increased adoption and acceptance of cloud-based processing. The world can benefit from cross-border data transfers while simultaneously ensuring the responsible processing and protection of that data.

To achieve this objective, the focus of privacy policy and regulation needs to be on the quality and effectiveness of the mechanisms and the controls maintained to protect the data in question. The accountability model, therefore, continues to be an important tool in increasing privacy and security by requiring entities to ensure that data will continue to be properly protected, regardless of where the data is located. The Act's support for the accountability model could be further strengthened by explicitly stating that data localisation is not required under the model.

Flexibility and Interoperability

Data protection and privacy frameworks that are based on a common set of international consensus-based principles contribute to global efforts in building interoperable systems and mechanisms that facilitate cross border data transfers while driving innovation and business investment in local markets. These mechanisms also help bridge current gaps in international privacy norms, while facilitating the safe and secure transfer of personal information. In the context of personal information protection, such mechanisms may include private codes of conduct, contractual arrangements such as standard contractual clauses (**SCCs**), certifications such as the APEC Cross Border Privacy Rules (**CBPR**) and Privacy Recognition for Processors (**PRP**), seals, or marks, and mutual recognition arrangements such as the adequacy with the European Union General Data Protection Regulation (GDPR). Some of these mechanisms are incorporated in other data protection frameworks to promote cross-border data flows, including the EU's General Data Protection Regulation, Singapore's Personal Data Protection Act, and Japan's Act on the Protection of Personal Information.

We encourage the Australian Government to recognise that many of the above-mentioned existing global mechanisms can meet the international data transfers requirements under the Act. Recognising these mechanisms as permissible means to transfer personal information across borders and implementing mechanisms such as the CBPR and/or PRP, would align the Act with global best practices. This will also allow businesses the flexibility to determine the mechanisms that will be best suited for different business scenarios.

In contrast, if the Australian Government were to create new data transfer mechanisms solely for use by companies transferring data from Australia, companies would lack the incentives to adopt those mechanisms and may see business and research initiatives drawn away from Australia to jurisdictions

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

which uphold and recognise other existing interoperable mechanisms that facilitate responsible data transfers. We encourage Australia to liaise with countries or regional blocs that integrate SCCs or regional certifications in their legislative frameworks, and aim for a situation in which an Australian SCC or regional certification could be mutually recognized or compatible with regional certifications.

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

We appreciate the opportunity to share these views and hope that they will be helpful as the Department considers its next steps on the Australian Privacy Act, promoting a robust data protection environment, while allowing responsible stewardship of data to continue benefiting the citizens and economy of Australia.

Please do not hesitate to contact us with any questions regarding this submission.

Sincerely yours,

Eunice Lim

Eunice Lim
Senior Manager, Policy - APAC
Global Data Alliance
eunicel@bsa.org