GLOBAL DATA ALLIANCE

COMMENTS ON THE PRIVACY ACT REVIEW REPORT 2022

Submitted Electronically to the Attorney-General's Department

The Global Data Alliance (**GDA**)[1] welcomes the opportunity to provide comments to the Attorney-General's Department's (**AGD**) Privacy Act Review Report 2022 (**Report**).[2]

I. Introduction

The GDA is a cross-industry coalition of companies that are committed to high standards of data privacy and security and that rely on the ability to transfer data responsibly across borders to support jobs and economic growth. Alliance members are active across 15+ sectors and over 150 countries. The GDA advances policies that promote the responsible handling of data without imposing unnecessary data localization mandates or restrictions on data transfers.

The ability to transfer data in a trusted and secure manner across transnational digital networks is important to many countries' policy objectives, including those relating to the protection of health, privacy, security, safety, and the environment. More specifically, data transfers play an important role in protecting or promoting cybersecurity,[3] economic development,[4] environmental sustainability,[5] innovation/intellectual property,[6] privacy/personal data protection,[7] regulatory compliance,[8] and small business promotion.[9]

The ability to transfer data across transnational digital networks is also critical to the functioning of numerous sectors[10] at every stage of the value chain.[11] This includes the agriculture,[12] automotive,[13] clean energy,[14] finance,[15] healthcare,[16] logistics,[17] media,[18] medical technology,[19] pharmaceutical,[20] and telecommunications[21] sectors. This ability supports shared economic prosperity:[22] 75 percent of the value of data transfers accrues to sectors such as manufacturing, agriculture, and logistics.

Finally, scientific and technological progress require the exchange of information and ideas across borders[23]: As the WTO has stated, "for data to flourish as an input to innovation, it benefits from flowing as freely as possible, given necessary privacy protection policies."[24]

As an organization focused on cross-border data policy, the GDA's recommendations focus on ensuring that the Act's treatment of international data transfers enhances cross border transfers with Australia. Although GDA members also have views on other sections of the Act, our members rely on other industry associations and organizations to present those views. Our specific comments follow.

II. Discussion re 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.[25] 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.[26] 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."[27]

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 data related to Australians. To avoid this result, GDA 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.[28]

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)

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).[29] 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).[30] 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.[31] 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.

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."[32] 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).[33] 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(2), 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 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."[34]

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."[35] 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.[36]

III. Conclusion

We appreciate the opportunity to share these views and hope that they will be helpful as the AGD 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,

Joseph Whitlock

Joseph P. Whitlock
Executive Director

---

[1] Global Data Alliance members are headquartered across the globe and are active in the advanced manufacturing, aerospace, automotive, electronics, entertainment, financial and payment services, health, consumer goods, supply chain, and telecommunications sectors, among others. BSA | The Software Alliance administers the Global Data Alliance. For more information, please see www.globaldataalliance.org

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

[3] Global Data Alliance, *Cross-Border Data & Cybersecurity* (2023), https://globaldataalliance.org/issues/cybersecurity/

[4] Global Data Alliance, *Cross-Border Data & Economic Development* (2023), https://globaldataalliance.org/issues/economic-development/

[5] Global Data Alliance, *Cross-Border Data & Environmental Sustainability* (2023), https://globaldataalliance.org/issues/environmental-sustainability/

[6] Global Data Alliance, *Cross-Border Data & Innovation* (2023), https://globaldataalliance.org/issues/innovation/

[7] Global Data Alliance, *Cross-Border Data & Privacy* (2023), https://globaldataalliance.org/issues/privacy/

[8] Global Data Alliance, *Cross-Border Data & Regulatory Compliance* (2023), https://globaldataalliance.org/issues/regulatory-compliance/

[9] Global Data Alliance, *Cross-Border Data & Small Business* (2023), https://globaldataalliance.org/issues/small-businesses/

[10] Global Data Alliance, The Cross-Border Movement of Data: Creating Jobs and Trust Across Borders in Every Sector (2020), https://globaldataalliance.org/wp-content/uploads/2021/07/GDAeverysector.pdf

[11] Global Data Alliance, *Global Data Alliance Infographic: Jobs in All Sectors Depend Upon Data Flows* (2021), https://globaldataalliance.org/wp-content/uploads/2021/07/infographicgda.pdf
[12] Global Data Alliance, *Cross-Border Data & Agriculture* (2022), at: https://globaldataalliance.org/sectors/agriculture/
[13] Global Data Alliance, *Cross-Border Data & Automotive Technology* (2022), at: https://globaldataalliance.org/sectors/automotive/
[14] Global Data Alliance, *Cross-Border Data & Energy* (2022), at: https://globaldataalliance.org/sectors/energy/
[15] Global Data Alliance, *Cross-Border Data & Finance* (2022), https://globaldataalliance.org/sectors/finance/
[16] Global Data Alliance, *Cross-Border Data & Healthcare* (2022), https://globaldataalliance.org/sectors/healthcare/
[17] Global Data Alliance, *Cross-Border Data & Supply Chain Logistics* (2022), https://globaldataalliance.org/sectors/supply-chain-logistics/
[18] Global Data Alliance, *Cross-Border Data & Media and Publishing* (2022), https://globaldataalliance.org/sectors/media-publishing/
[19] Global Data Alliance, *Cross-Border Data & Medical Technologies* (2023), https://globaldataalliance.org/sectors/medical-technology/
[20] Global Data Alliance, *Cross-Border Data & Biopharmaceutical R&D* (2022), https://globaldataalliance.org/sectors/biopharmaceutical-rd/
[21] Global Data Alliance, *Cross-Border Data & Telecommunications* (2022), https://globaldataalliance.org/sectors/telecommunications/
[22] Global Data Alliance, *Cross-Border Data Transfers & Economic Development: Access to Global Markets, Innovation, Finance, Food, and Healthcare* (2021), https://globaldataalliance.org/wp-content/uploads/2021/07/05062021econdevelopments1.pdf
[23] Global Data Alliance, *Cross-Border Data Transfers & Innovation* (2020), https://globaldataalliance.org/wp-content/uploads/2021/07/04012021cbdtinnovation.pdf
[24] WTO, Government Policies to Promote Innovation in the Digital Age, 2020 World Trade Report (2020), at: https://www.wto.org/english/res_e/booksp_e/wtr20_e/wtr20-0_e.pdf
[25] Report (2023), p.1.
[26] Report (2023), p. 236-237.
[27] Report (2023), p. 236.
[28] Report (2023), p. 236.
[29] Report (2023), p. 247.
[30] 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
[31] Report (2023), p. 239.
[32] Report (2023), p. 239.
[33] Report (2023), p. 240-241.
[34] Report (2023), p. 241-242.
[35] Report (2023), p. 241.
[36] Report (2023), p. 241.