23 February 2024

Global Data Alliance Comments on
Senate Inquiry into Sovereign Capability in the Australian Tech Sector

Submitted to the Senate Standing Committee on Finance and Public Administration

The Global Data Alliance (**GDA**)[1] welcomes the opportunity to submit comments to the Senate Standing Committee on Finance and Public Administration (**Committee**) on its inquiry into supporting the development of sovereign capability in the Australian tech sector (**Inquiry**).[2]

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 Inquiry's Terms of Reference[3] raise important considerations, including the need to support Australian technology companies and the consequences of using "non-sovereign" tech in the Australian Public Sector (**APS**). Recognizing this objective, it is also important to ensure that the Australian public and private sector alike maintain seamless cross-border access to knowledge, information, data, and digital tools from trusted partners across world. This access is critical to myriad policy objectives, ranging from technology-specific priorities such as digital transformation and cybersecurity threat management to broader national and societal priorities relating to the economy, environment, finance, health, safety, and security. The GDA urges the Committee to avoid unintended impacts on these priorities through the types of self-defeating data localization mandates and cross-border data transfer restrictions that have hampered the growth and resilience of other leading economies, including China.

The ability to transfer data across transnational digital networks is critical not only to maintaining and enhancing sovereign capability in the APS, but also to other important Australian policy objectives, including those relating to the protection of cybersecurity,[4] economic development,[5] environmental sustainability,[6] innovation/intellectual property,[7] privacy/personal data protection,[8] regulatory compliance,[9] and small business promotion.[10] Please see Annex I for additional details on the importance of cross-border data in protecting Australian cybersecurity.

The ability to transfer data across transnational digital networks is also critical to many APS functions, including in relation to agriculture,[11] clean energy,[12] finance,[13] and health[14] / [15]. Finally, scientific and technological progress require the exchange of information and ideas across borders[16]: 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."[17] Please see Annex II for additional details on the importance of cross-border data in protecting other APS activities and priorities.

We hope that our comments will assist the Committee with this Inquiry. Please do not hesitate to contact me if you have any questions regarding this submission or if I can be of further assistance.

Sincerely,

Joseph P. Whitlock

Executive Director

Annex I

Importance of Cross-Border Data & Digital Trade to Australian Cybersecurity

Cross-border data transfers are critical to cybersecurity in part because they allow for cybersecurity tools to monitor traffic patterns, identify anomalies, and divert potential threats in ways that depend on global access to real-time data. Additionally, companies may choose to store data at geographically diverse locations to obscure the location of data and reduce risk of physical attacks, to enable companies to reduce network latency, and to maintain redundancy and resilience for critical data in the wake of physical damage to a storage location. Conversely, when governments mandate localization or restrict the ability to transfer and analyze data in real-time, they create unintended vulnerabilities, as summarized below:

- **Data Transfers & Integrated Cybersecurity Planning.** Data transfer restrictions and localization requirements force organizations to adopt a siloed approach to data, often restricting the locus of certain data, but not others. This differentiation creates unnecessary technical complexity without any corresponding benefit to security. Simply put: artificial requirements to store data within borders strain the people, processes, and technologies an organization needs to manage its cybersecurity risk.

- **Data Transfers & Cybersecurity Awareness.** Data transfer restrictions and localization requirements impede visibility of cybersecurity risks, not only at the intra- and inter-organizational levels, but also at national and international levels. If cyber defenders cannot access threat indicators or other cybersecurity data collected in one jurisdiction, it becomes harder to address malicious cyber activity in other jurisdictions.

- **Data Transfers & Cybersecurity Collaboration.** Data transfer restrictions and localization requirements can impede cross-border collaboration, information sharing, and other coordinated network defense. When such restrictions and requirements isolate network defenders from each other, they cannot adopt a unified and coordinated defensive posture against malicious actors that do not respect national borders. In short, data transfer restrictions can give malicious actors that do not respect local legal requirements a lasting structural advantage over cyber defenders that do.

- **Data Transfers & Third-Party Cybersecurity Services.** Many organizations amplify their own cybersecurity risk management through third-party cybersecurity service providers. Best-in-class services depend on access to cyber data from around the globe. Without this access, these services and their users become more vulnerable to compromise.

- **Data Transfers & Cybersecurity Resiliency.** Whether a particular geographic area is at high risk for a natural disaster or in a potential future war zone, having data efficiently distributed is a crucial component of resiliency. The misconception that keeping data only within national boundaries will increase its security can actually create significantly more risk.

- **Data Transfers & Protectionism in the Name of Cybersecurity.** Localizing data within a country—or blocking its transfer—has no functional cybersecurity benefit. Security is determined by the technical and operational protections that accompany the data, not the location. Transfer restrictions and localization requirements are often used to advance other objectives. Perhaps the most systemic problem with using cybersecurity laws to require localization, then, is that it diminishes the role of laws and policies that are truly designed to improve security.

Annex II

Importance of Cross-Border Data & Digital Trade to Australian Public Sector Priorities

Cross-border access to information and data transfers are critical for numerous objections, operations, and functions of the APS. This includes:

1. **Artificial Intelligence:** Meeting APS goals relating to AI research in vital areas like healthcare and climate change, which depend upon ensuring continued Australian cross-border access to high quality data from around the world.

2. **Cyber- and Homeland Security**: Cyber-defenders across the APS cannot protect Australian networks without cross-border access to global cyberthreat intelligence. Likewise, Australian border authorities depend upon cross-border digital access to international supply chain threat intelligence to interdict dangerous imports various border enforcement programs.

3. **Economy:** Australian commercial and trade authorities depend upon cross-border access to information regarding business, sales, and export opportunities available to Australian citizens.

4. **Environment**: Australian environmental authorities depend upon cross-border access to satellite, meteorological, emissions, and other data from across the globe to advance efforts at combatting climate change and promoting a sustainable environment.

5. **Finance**: Australian financial authorities depend on cross-border access to financial information flows to combat terrorist financing, money laundering, corruption and fraud. Securities and tax authorities also require ready cross-border access to financial information to fulfill their respective statutory functions.

6. **Foreign Policy**: Australians Department of Foreign Affairs and Trade relies on cross-border data transfers for every aspect of its work in advancing Australian foreign policy, interests, and security abroad. This extends to efforts to negotiate trade agreements, defend human rights, and promote foreign economic development.

7. **Health & Safety:** Australia's health authorities depend upon reliable cross-border access to health data in many contexts. This includes maintaining cross-border access to pre-clinical and clinical trial data from around the world to evaluate new treatments and healthcare solutions. It also includes real-time access to global epidemiological statistics and pandemic-related indicators to protect Australia's population from emergent health risks. It also includes cross-border access to scientific publications and laboratory results from around the world to promote scientific advances, as well as cross-border access to pricing data for healthcare delivery purposes.

8. **Innovation & IP:** IP Australia and other innovation and IP-focused agencies in Australia depend on cross-border access to data on inventions, creations, and R&D from abroad, including to assess prior art, registrability, and ownership of IP, as well as foundational research across the sciences.

[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] Inquiry into supporting the development of sovereign capability in the Australian tech sector, December 2023, https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Finance_and_Public_Administration/Supporting_Aust_tech47.

[3] Terms of Reference for inquiry into supporting the development of sovereign capability in the Australian tech sector, December 2023, https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Finance_and_Public_Administration/Supporting_Aust_tech47/Terms_of_Reference

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

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

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

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

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

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

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

[11] Global Data Alliance, *Cross-Border Data & Agriculture* (2022), at: https://globaldataalliance.org/sectors/agriculture/

[12] Global Data Alliance, *Cross-Border Data & Energy* (2022), at: https://globaldataalliance.org/sectors/energy/

[13] Global Data Alliance, *Cross-Border Data & Finance* (2022), https://globaldataalliance.org/sectors/finance/

[14] Global Data Alliance, *Cross-Border Data & Medical Technologies* (2023), https://globaldataalliance.org/sectors/medical-technology/

[15] Global Data Alliance, *Cross-Border Data & Biopharmaceutical R&D* (2022), https://globaldataalliance.org/sectors/biopharmaceutical-rd/

[16] Global Data Alliance, *Cross-Border Data Transfers & Innovation* (2020), https://globaldataalliance.org/wp-content/uploads/2021/07/04012021cbdtinnovation.pdf

[17] 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