10 June 2022

Mr Brendan Dowling
First Assistant Secretary
Digital and Technology Policy Division
Department of Home Affairs
AUSTRALIA

Dear Brendan,

Consultation on Australia's National Data Security Action Plan

Visa welcomes the opportunity to contribute to fostering a robust approach to data security in Australia. We are pleased to provide our views in response to the Discussion Paper (the Discussion Paper) for consultation on the development of Australia's National Data Security Action Plan (the Action Plan).

Trust underpins everything at Visa — our network, partnerships, payment platforms, and our approach to data-driven innovation, which we believe should benefit consumers and payments ecosystem participants in privacy-protective ways. Our core business is founded on Visa's ability to create trusted data-sharing relationships between financial institutions that facilitate digital commerce in a secure, safe, and convenient way for consumers and businesses. Safeguarding those who use our products, services, and network is Visa's highest priority. As an international business dedicated to security, we commend the Department of Home Affairs (Home Affairs) for its focus on national data security.

In responding to the Discussion Paper, we have focused on the three questions below, numbered to align with the question order in the Discussion Paper. Our response illustrates how Visa believes the Australian Government can approach data security in a manner that is interoperable with existing international frameworks and policy measures, and which allows Australian citizens to continue to benefit from cross-border data flows.

Q2. How can Australian Government guidance best align with international data protection and security frameworks? Are there any existing frameworks that you think would be applicable to Australia's practices (e.g., the European Union's General Data Protection Regulation)?

Visa AP (Australia) Pty Ltd
Level 39, International Tower Two
200 Barangaroo Avenue
Barangaroo NSW 2000
Australia
ABN 20 134 885 564

www.visa.com.au

In relation to existing international data protection frameworks, the European Union's (EU) General Data Protection Regulation (GDPR) is the framework that is most applicable to Australia's current data protection and future reforms. Since coming into effect in May 2018, GDPR has set the global standard for accountability-based data protection models and has had a seminal influence on the development of new privacy legislation in a number of countries (e.g., New Zealand's Privacy Act 2020) as well as the reform of existing privacy laws in other countries (e.g., Canada, Japan and Singapore).

Data protection and privacy frameworks that are based on a common set of international consensus-based principles help global efforts to build interoperable systems and mechanisms that facilitate cross-border data transfers. These coordination mechanisms also help to bridge current gaps in international privacy norms, while facilitating the safe and secure transfer of personal information.

This accountability-based approach requires organisations to adopt appropriate and comprehensive technical measures and organisational safeguards regarding all aspects of their data processing activities. In addition, this approach requires organisations to demonstrate the existence and effectiveness of such measures, rather than imposing prescriptive and onerous requirements. GDPR also encourages a "privacy by design" approach under which organisations ensure that their products and services take privacy requirements into account – from inception and throughout the data lifecycle.

While Australia's data protection and security laws (such as the Privacy Act 1988) already follow a flexible and principles-based approach towards data protection, there are definite advantages in increasing the alignment between these laws and GDPR. Visa notes the ongoing review of the Privacy Act in Australia, including the most recent public consultation by the Attorney-General's Department[1], in which a number of further reforms were proposed. We support these proposed reforms and the opportunity that they present to achieve greater alignment with GDPR.

More specifically, there are a number of areas where there is potential for greater alignment between Australia's laws (including the Privacy Act) and GDPR, including:

Controller/processor distinction – GDPR and many other privacy laws clearly define the different roles of data controllers and processors. This clear allocation of accountability between data controllers and processors allows their privacy obligations to be determined based on their respective levels of responsibility and control, specifically in key areas such as the exercise of data subject rights and breach notification. Adopting this distinction would improve alignment between Australia and other jurisdictions as well as facilitating compliance by international companies.

[1] Attorney-General's Department, Privacy Act Review – Discussion Paper, October 2021, https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/user_uploads/privacy act-review-discussion-paper.pdf

Legal bases – Australia's data protection laws should include recognition of a range of alternative legal bases for processing on which companies can rely, based on the most appropriate option in each context. We recommend these alternative bases include the principle of "legitimate interests" (i.e. the principle that data may be processed based on an assessment of the respective interests and rights of data controllers and data subjects and the necessity of processing), in line with Article 6(1)(f) of GDPR. This will ensure consistency for international companies and facilitate their ability to transfer personal information internally between related entities.

Security requirements – GDPR is also notable for its inclusion of detailed security principles. These principles explicitly reference the factors which are relevant in determining what is required to take "reasonable" or "appropriate" security measures. As considered within Section 19 of the Attorney-General's Department's recent consultation paper on the Privacy Act, a high-level and inclusive list of such factors (consistent with existing Australian Privacy Principles Guidelines on security) could be included in the Privacy Act. This would codify the interdependency between information security and privacy and clarify compliance requirements for organisations.

Data breach notification – Visa sees value in further harmonising Australia's Notifiable Data Breaches scheme under the Privacy Act for consistency with other domestic notification schemes (e.g., under the Security of Critical Infrastructure Act 2018 and the Australian Prudential Regulation Authority Prudential Standard CPS 234 (Information Security)). There may also be benefit in revising the scheme to align with international, risk-based frameworks by ensuring that organisations are given sufficient time to fully assess the impact of any breach and take appropriate remedial action, while streamlining their reporting obligations where possible.

Cross-border transfers – The need to ensure greater consistency and interoperability between the Privacy Act and the privacy regimes of other countries is particularly important in relation to cross-border data transfers. Data is not contained by geographical borders and alignment with overseas regimes is essential to facilitate cross-border transfers of information within the global digital economy, while advancing innovation and international trade. There are several independent mechanisms that have been implemented under GDPR Article 46, such as Binding Corporate Rules and Standard Contractual Clauses, to ensure the safe transfer of data. Recognising a range of mechanisms to be utilised on a voluntary and flexible basis would help accommodate different business models, while promoting security, service reliability, business efficiency and facilitating (rather than impeding) data flows. Similar mechanisms have been implemented in many other countries, including those (such as New Zealand) that have been recognised as offering levels of protection that are essentially equivalent to the EU, thereby satisfying GDPR adequacy requirements. We suggest that the Australian Government consider these mechanisms as an integral part of any review aimed at achieving greater alignment of privacy and data security laws between Australia and other jurisdictions.

Another well-established and widely recognised framework that enables cross-border transfer of data is the APEC Cross-Border Privacy Rules (CBPR) System, in which Australia participates. Visa sees value in consideration also being given to Australia's participation in the broader Global Cross-Border Privacy Rules Forum that was established in April 2022 by a number of other APEC members. The resulting international certification system that will be established, based on (but separate from) the APEC CBPR System, will support the free flow of data and promote greater interoperability between privacy frameworks by enabling participation by a far broader range of non-APEC jurisdictions. While reliance on any certification process should be voluntary to allow organisations to demonstrate compliance in other ways, this process could be complemented by the recognition of other international industry standards and best practices (e.g., PCI-DSS, discussed below) as a basis for secure management and transfer of information. This would assist in facilitating the compliance of stakeholders.

Q4. How could Australian legislative and policy measures relating to data security be streamlined to better align with your obligations in international jurisdictions? Does variation in international approaches create hurdles to your effective participation in the global market?

a. What obligations are you most commonly subjected to from international jurisdictions?

Australian legislative policy measures relating to data security could be streamlined to better align with obligations in international jurisdictions, by recognising that many organisations such as Visa already meet internationally-recognised standards.

As a global payment system operator, Visa is subject to regulatory oversight in the United States by the Federal Financial Institutions Examinations Council (FFIEC). Regulators around the world recognise this robust regulatory oversight in the U.S. and, as such, do not place duplicative oversight frameworks on Visa.

In terms of global standards and obligations, Visa has incorporated a number of these into our policies and framework, including the Payment Card Industry (PCI) Data Security Standards (DSS) for securing payment data both in the physical and digital space. We detail some of these obligations below.

Regulatory harmonisation goes beyond technical rules to ensure policies and regulations can work in tandem. For example, many potential data security-related concerns, including the secure treatment of personal information and consumer permissioning, can be addressed through existing consumer privacy and data protection regulation. This is particularly the case if such regulation is principles-based and properly agile to extend to new use cases. The creation of separate legal standards and regulatory enforcement mechanisms, especially within one country, can result in compliance challenges for companies and regulators, as well as uncertainty for consumers.

Importantly, discussions on interoperability alone can sometimes result in system-wide standardisation and uniformity. Such an outcome can hinder competition and stifle

innovation. As a result, it is very important that regulatory stakeholders find a balance between achieving harmonisation to allow for effective participation and compliance in the global market and continuing to facilitate an environment that enables competition and product differentiation.

When successfully achieved, interoperability may feel "seamless," but the process requires coordination and agreement across a broad range of stakeholders and, therefore, can be quite complex. Visa works closely with participants in the global payments ecosystem to enable multiple layers of security to support secure and seamless payment experiences. The use of global standards is a key pillar to how we provide this service.

As referenced briefly above, Visa's approach to data security is based on the Payment Card Industry (PCI) Data Security Standards (DSS), a global information security standard designed to prevent fraud through increased control of card data. PCI-DSS compliance is required of all entities that store, process, or transmit Visa cardholder data, including financial institutions, companies, and service providers. Visa's programs manage PCI-DSS compliance by requiring that participants demonstrate compliance on a regular basis.

The Payment Card Industry Security Standards Council (PCI SSC) has published version 4.0 of the PCI-DSS, which provides a baseline of technical and operational requirements designed to protect cardholder data. This version's improvements are intended to support the needs of the payment industry to protect against evolving threats. The four main goals for version 4.0 set by the PCI SSC, and some examples of the changes introduced, are outlined below:

1. Continue to meet the security needs of the payments industry
    a. Expanded multi-factor authentication requirements
    b. Updated password requirements
2. Promote security as a continuous process
    a. Clearly assigned roles and responsibilities for each requirement
3. Add flexibility for different methodologies
    a. Customised implementation approach introduced for validating PCI-DSS requirements
4. Enhance validation methods
    a. Increased alignment between Report on Compliance, Self-Assessment Questionnaire, and Attestation of Compliance

The PCI Software Security Framework (PCI SSF) is a collection of standards and programs for the secure design and development of payment software. The PCI SSF program is similar to and will replace the Payment Application Data Security Standard (PA-DSS) when the standard is retired at the end of October 2022.

As background, Visa developed the Payment Application Best Practices (PABP) in 2005. We did so to provide software vendors with guidance in developing payment applications that help companies and agents mitigate compromises, prevent storage of sensitive cardholder data (i.e. full magnetic stripe data, CVV2 or PIN data), and support overall compliance with the PCI-DSS. In 2008, the PCI SSC adopted Visa's PABP and released the standard as the PA–DSS, which has since replaced PABP for the purpose of Visa's compliance program.

Q5. Does Australia need an explicit approach to data localisation?

Visa commends Home Affairs for taking a balanced, thoughtful approach to data localisation in Australia. Data is a lynchpin of the modern, global economy. However, data on its own holds limited value. It is data *flows* that create insights that deliver value to citizens and economies.

Open, global, interoperable networks power the world by enabling the free flow of information and commerce. They allow a plane to fly safely from Sydney to Dubai, keep our phones working almost anywhere, and allow a credit card from a bank in Spain to function seamlessly at a restaurant in Perth. The benefits they deliver to citizens around the world are profound.

The free flow of data across borders also benefits broader economies in many ways – it improves productivity, lowers costs for consumers, and boosts employment.[2] Cross-border data flows, digital services, and associated technologies are critical to the future growth of the global economy. For example, cross-border data flows allow local companies to take advantage of data infrastructure outside of Australia, bringing new and enhanced services that will, in turn, aid economic growth.

When cross-border data flows are fragmented, such as in the event of data localisation measures, these benefits are eroded. Overly restricting data flows increases security, operational, and fraud risks and dampens innovation. Fraud detection relies on companies being able to track and analyse suspicious transactions across national borders, thereby increasing security and stability in the payments ecosystem. Any regulation that fragments a company's data analysis or visibility into global data undermines these advanced capabilities and increases fraud in the ecosystem. In such a situation, companies will be forced to rely more heavily on local patterns than on global ones, making risk models less powerful and consumers less secure.

[2] For example, the World Bank believes removing restrictive data policies can help countries achieve a 4.5 percent increase in productivity. See World Development Report 2020: Trading for Development in the Age of Global Value Chains, October 2019, p.244. Available at https://documents.worldbank.org/en/publication/documents-reports/documentdetail/310211570690546749/world-development-report-2020-trading-for-development-in-the-age-of-global-value-chains.

Furthermore, data localisation often prevents businesses from adequately ensuring data resilience, data recovery, and business continuity by severing connections with key data centres around the world.[3] Many international businesses have operating models and global data centres to ensure operational resilience. Leveraging any one of a number of global data centres – and falling back on a different centre if one is unavailable – is key to operational resilience. Requiring data storage and processing on a local server can lead to a "single point of failure" and leave the entire payments ecosystem vulnerable. If a single data centre is unavailable, without fall-back capability to other data centres, it risks halting the entirety of an economy's payments ecosystem.

For these reasons, Visa encourages Home Affairs to continue taking a balanced approach to data localisation that supports free, open and secure cross-border data flows. We commend the Action Plan for its objectives "to contribute to priority initiatives such as international data standards, and data flows that are safe, secure, lawful, ethical, and in line with Australia's values and interests."[4] The choice between security and free data flows is a false one. For data use to be equitable, trusted and safe, it is necessary to achieve both data security *and* openness – and we can.

High-quality and inclusive digital trade agreements that ensure interoperability, allow data to move freely across borders and promote a level playing field are essential to enable access to world-class technologies and contribute to sustainable and equitable economic growth. As noted in the Action Plan, "widespread local storage requirements can represent significant barriers to trade and economic cost."[5] Digital trade generates and enables global value chains – supporting a wide range of sectors and stakeholders and operating seamlessly across national borders. Visa believes that digital trade agreements represent a powerful and strategic tool to unlock the benefits of digital trade and establish cross-border standards for the flow of data, including trade in electronic payment services.

We welcome that the Action Plan reiterates Australia's commitment to digital trade agreements, such as the Australia-Singapore Digital Economy Agreement (DEA). The DEA is one of the most comprehensive digital trade agreements to date and it serves as a global example of positive measures that strengthen data security and technological collaboration as well as spurring innovation, all while protecting personal data. We note that the DEA also commits to regulatory collaboration and cooperation in Artificial Intelligence (AI), digital identity, and personal data protection, areas in which such commitments will be critical to promote interoperability and innovation.

[3] Joshua P. Meltzer and Peter Lovelock, "Regulating for a digital economy: Understanding the importance of cross-border data flows in Asia," The Brookings Institution, March 2018, pp. 19-22. Available at https://www.brookings.edu/wp-content/uploads/2018/03/digital-economy_meltzer_lovelock_working-paper.pdf.

[4] Department of Home Affairs, National Data Security Action Plan, page 20.

[5] Department of Home Affairs National Data Security Action Plan, page 20. Available at National Data Security Action Plan (homeaffairs.gov.au)

Visa has appreciated the opportunity to contribute to this consultation and to share our perspectives on the National Data Security Action Plan. We would welcome the opportunity to discuss any of these comments in more detail or to address any queries regarding our submission.

Yours sincerely,

Julian Potter
Group Country Manager, Australia, NZ & South Pacific

About Visa

Visa is the world's leader in digital payments. Our mission is to connect the world through the most secure, reliable, and innovative payment network – enabling individuals, businesses, and economies to thrive. Our advanced global processing network, VisaNet, provides secure and reliable payments around the world, and is capable of handling more than 65,000 transaction messages a second.

In Australia, Visa has offices in Sydney and Melbourne. Together with our Australian financial institutions, fintech and business clients, and our technology partners, we are committed to building a future of commerce that fosters Australian economic growth, security and innovation.

Visa continues to expand acceptance across the payments ecosystem, ensuring that every Australian can not only pay, but also be paid in a convenient and secure way. In fact, from 2015-19, Visa invested nearly US$9 billion in systems resilience, fraud management and cybersecurity, including tokenisation, Artificial Intelligence (AI) and blockchain-based solutions, to bring even more security to every transaction[6]. In 2021, Visa's AI-driven security helped financial institutions prevent more than AU$354 million in fraud from impacting Australian businesses[7].

As commerce moves rapidly online, Visa recently released its updated Australian Security Roadmap 2021-23[8] in response to the increasing risk of cybercrime and scams facing Australian businesses and consumers. The roadmap highlights the steps that Visa, together with industry, are taking to continue to secure digital payments in Australia, including:

- Preventing enumeration attacks through new ecommerce requirements
- Driving adoption of secure technologies
- Securing digital first payment experiences, including contactless ATM access
- Enhancing the cybersecurity posture of payments ecosystem participants
- Preventing Australian consumers and businesses from becoming victims of scams
- Ensuring payments ecosystem resilience through real-time AI solutions.

The Australian Security Roadmap 2021-23 is available here.

[6] Visa (2019), US$9 billion investment figure based on internal data on global technology and operations investments between FY2015-FY2019. More information is available here.
[7] Visa (2021), Visa's AI prevents more than $350 million in fraud from disrupting Australian businesses.
[8] Visa (2021), Security Roadmap 2021-23: Securing the Commerce Ecosystem in Australia.