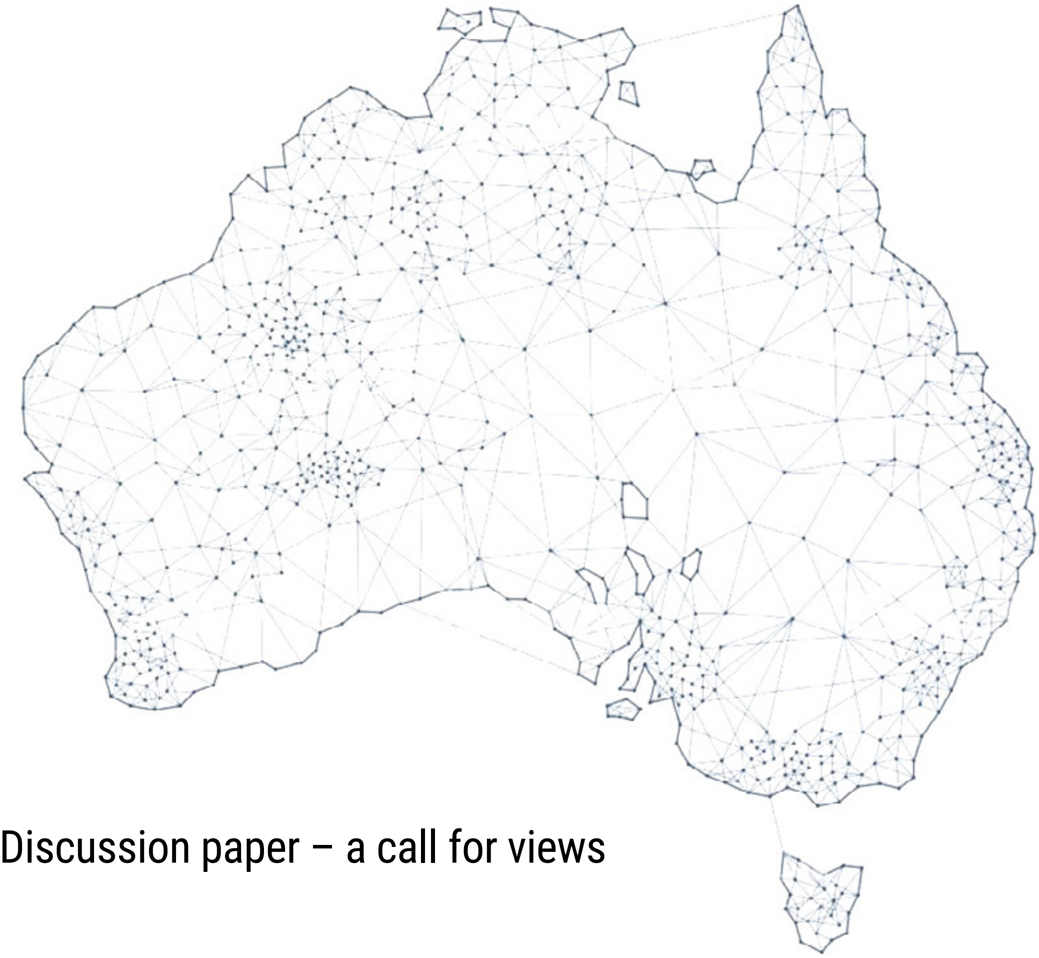
Australian Government

NATIONAL DATA SECURITY ACTION PLAN



Discussion paper – a call for views

WHO SHOULD READ THIS PAPER?

This Discussion Paper focuses on data security policy settings for state and territory governments, industry and the broader economy. The security of individuals', organisations', and governments' data is important for all Australians. We welcome responses from all Australians to inform the National Data Security Action Plan's direction. Submissions can be made through the Department of Home Affairs at: https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/data-security.

What is data?

Data is any information in a form capable of being communicated, analysed or processed (whether by an individual or by computer or other automated means).[1]

- Data can include personal information, which is information about an individual or an individual who is reasonably identifiable – such as their basic contact details, records generated through their interaction with services or the internet, or information about their biometrics (physical or behavioural characteristics). Data can also include population-level data, such as demographics.
- Data can include information that can be used to describe location (such as geospatial reference details) or the environment (such as biodiversity or the weather). It can also refer to the information captured or generated by the networks of sensors that make up the Internet of Things.
- Data about systems can include administrative records about businesses and public services.

What is data security?

Data security is a broad term that refers to protecting the information collected, processed, and stored on digital systems and networks.[2]

What is the difference between privacy and data security?

Privacy and data security combine to ensure the protection and security of data. Privacy settings ensure the protection and security of **personal and sensitive information** including from unauthorised access. Data security seeks to address unauthorised access to **all** data types.

[1] Consistent with the Australian Data Strategy and the Data Availability and Transparency Bill

[2] Consistent with the Australian Cyber Security Centre's definition of data security

CONTENTS

MINISTER’S FOREWORD

Data has never been more valuable – it is an increasingly important driver of growth in our modern economy. Whether about individuals, businesses or government, data underpins how we communicate, conduct business, and receive services. At the same time, it can be stolen, manipulated or used as a weapon by foreign adversaries and criminals. As Australia seeks to harness opportunities created by digital technologies and to grow the digital economy, it is essential that appropriate data controls and accountability mechanisms are in place to enable a prosperous and secure Australia.

Data is a strategic asset. Increasingly, foreign adversaries and malicious actors seek to exploit and leverage Australian data as a means to undermine our security, prosperity and social cohesion. We have witnessed aggregated data used to build psychological, financial or personal profiles, and identify individuals vulnerable to exploitation or radicalisation. Insecure data is expensive. Data breaches cost businesses an average of $3.9 million in 2021, an increase of over 30 per cent from 2020, and the highest average cost in the last 17 years.[3]

The Australian Government is seeking your help to improve data security measures and close the gaps that exist in our data settings. We want to ensure that governments, businesses and communities are informed and resourced to protect their data. This is why I am committed to delivering Australia’s first National Data Security Action Plan (Action Plan).

The Australian Government is investing to strengthen security and build resilience in infrastructure that underpins our digital economy. This includes the *Security Legislation Amendment (Critical Infrastructure) Act 2021*, which will deliver greater accountability and responsibility requirements for entities within the data storage or processing sector.

[3] Cost of a Data Breach Report 2021 - Australia | IBM

In May 2021, the Australian Government announced a $1.2 billion investment in Australia's digital future through the Digital Economy Strategy as part of the 2021-22 Federal Budget. It includes a range of initiatives to support the growth of our digital economy including enhancing the security of Australia's data, including the recently launched Australia Data Strategy.

The Action Plan will deliver a whole-of-economy approach to data security, complementing the Government's work to strengthen Australia's cyber security regulations and incentives by setting clear cyber security expectations; increasing transparency and disclosure; and protecting consumer rights. The Action Plan will provide Australian individuals and businesses with the trust and assurance required to make Australia a top 10 digital economy by 2030.

I encourage all Australians to have a say in how our data is secured.

Karen Andrews

Karen Andrews
Minister for Home Affairs

INTRODUCTION

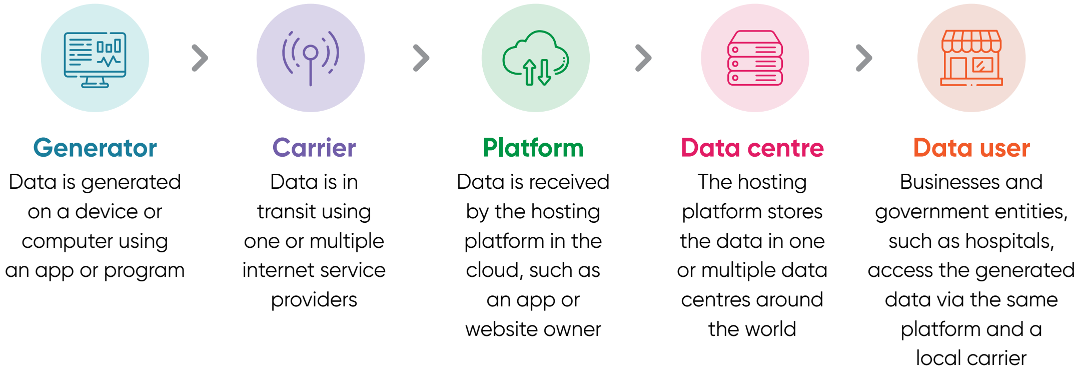
Australian government, business and citizen data is a strategic asset and must be secured accordingly. Data is fundamental to how we work, relate and recreate. It is used to process bank transactions, manage payrolls for our businesses, stay in touch with friends, confirm our vaccination status and run the machines and infrastructure that are essential to our way of life.

Data and digital technologies have become a critical part of our economy and the security of our data is critical to Australia's national interest. This includes information such as biometric information used to prove an individual's identity through facial recognition, which Australians increasingly use to make their online activity more secure.

The significant growth in data generation over the past decade has resulted in a commensurate uptick in the growth of data driven industries such as data centres, cloud service providers and digital platforms which commoditise data through aggregation (Google, Facebook, TikTok etc.). This is largely the result of huge advancements in the accessibility, transfer, processing and storage of large volumes of data. Data is increasingly mobile. Rather than storing data on your phone, computer or a server in your office, it is now often stored and processed across multiple locations and by multiple vendors.

The heightened level of connectivity and movement of data is a net positive for the economy and society. It has allowed faster, more consistent service delivery and removed distance as a barrier for businesses and personal correspondence. It can also have security benefits, with cloud adoption transferring the burden of cyber security from individuals and small businesses to a cloud service provider better equipped to manage cyber threats. None of these benefits, however, can be realised if the legislative and policy settings are not fit for purpose. Additionally, while businesses and government are the most impacted by the significant shift in the way data is processed and stored, individuals also have rights, roles and responsibilities when it comes to ensuring their data is secure.

Figure 1 – A simplified view of data movement



Generator
Data is generated on a device or computer using an app or program

Carrier
Data is in transit using one or multiple internet service providers

Platform
Data is received by the hosting platform in the cloud, such as an app or website owner

Data centre
The hosting platform stores the data in one or multiple data centres around the world

Data user
Businesses and government entities, such as hospitals, access the generated data via the same platform and a local carrier

It is vital that as a nation, we remain on the front foot to ensure all Australian governments, businesses and individuals know how their data is managed, stored and secured. As Australia's economy increasingly digitises, the volume and value of data commensurately grows. This presents the need for a consistent whole-of-economy approach to data security.

The Australian Government recognises that the existing data security regulatory environment is complex and contested, with many different initiatives targeting different sections of the economy. For example, there is no national standard for assessing and marking the sensitivity of government data holdings — each jurisdiction has its own security classification system — and in turn, no common standard for the protection of similar data sets held by different jurisdictions. This makes it difficult for governments and businesses to map and adhere to the relevant requirements and standards.

To simplify, educate, and improve national data security, the Australian Government is developing Australia's first National Data Security Action Plan (the Action Plan) to deliver whole-of-economy expectations and requirements for data security.

The Action Plan will set out a coordinated approach, providing proportionate data security expectations across the economy, underpinned by three principles for data security – Secure, Accountable and Controlled. The Action Plan will align and build on existing data security settings across the economy and build on existing Australian Government initiatives such as Australia's Cyber Security Strategy 2020 and Australia's first Data Strategy in support of the Digital Economy Strategy.

In developing the Action Plan the Australian Government will consider all aspects of the current data security settings in Australia including:

- How to strengthen and coordinate data security across the broader economy.
- Measures to ensure data of all Australians is appropriately controlled and accountable.
- Ensuring all Australians know their rights, roles and responsibilities when it comes to the secure handling, storing and managing of data.
- Ensuring data security guidance, in both policy and legislation, is consistent between Federal and state and territory governments.
- Promoting alignment across data security requirements established under other data and digital initiatives, including the Consumer Data Right and the Data Availability and Transparency Bill.
- Outlining our international data security obligations and the risks posed to national security if of our data is misused by foreign actors or cyber criminals.
- Policy options to support whole of economy data security uplift and digitalisation as we work towards becoming a top 10 digital economy by 2030.

This discussion paper focuses on policy settings for state and territory governments, businesses and the broader economy and we seek your views as to how the Australian Government can best achieve data security uplift at a national level.

Submissions can be made up through the Department of Home Affairs website at: https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/data-security.

WHY DO WE NEED TO PROTECT OUR DATA?

Australia's data is a valuable national asset requiring robust security settings

The storage, access and management of data has significant strategic, economic and national security implications. Data is essential to our national security priorities, to the growth of our economy, to the delivery of services and, ultimately, our way of life. It can be a currency, a national security vulnerability, and a weapon used against individuals, businesses and governments. The COVID-19 pandemic has accelerated the need to better protect our data as more and more Australians shift online. To enable Australians to engage with confidence online, governments, businesses and individuals need to know and trust that their data is secure.

Inadvertently allowing another country to access Australia's most critical data will erode our sovereignty and control over that data in the long term. From a national security perspective, aggregated 'big data' needs to remain available in order to harness the opportunity it presents; however, effective and robust measures to protect data are essential. Open source reporting has observed foreign powers actively seeking to gain access to data that is valuable, such as intellectual property, to gain strategic and commercial advantages as highlighted in the case study below. Data is also a key vehicle to enable countries to progress geo-political agendas. This includes non-likeminded countries who wish to do us harm or access Australian data as a means to conduct espionage or foreign interference. Prioritising security in the application and use of data is vital to ensure the protection of our most valuable data from foreign adversaries.

CASE STUDY

2021 MICROSOFT EXCHANGE COMPROMISE

In July 2021, the Australian Government publicly acknowledged that China's Ministry of State Security (MSS) had hacked Microsoft Exchange software – enabling the compromise of tens of thousands of computers globally. The MSS then stole intellectual property to provide commercial advantage to the Chinese Government. Stolen intellectual property is alleged to include information belonging to the public and private sectors. The US and UK governments noted that private sector victims were heavily targeted and that the compromise reflected a pervasive pattern of behaviour by Chinese state-backed cyber groups.

Data is a valuable resource

The emergence of new technologies such as quantum computing, super computers and artificial intelligence (AI), coupled with the increased digitalisation of the global economy has made data of Australians more abundant, available and easier to integrate. From analytics of purchasing behaviours, to research into health outcomes, to refining business and government services, the ability to quickly process large volumes of data for insights has resulted in a strong appetite for data for both legitimate and illegitimate reasons. Data is an increasingly important driver of growth for Australia's modern connected economy, helping consumers, businesses and governments make better decisions. *Figure 2* details examples of situations where data can be used to positive effect.

All levels of government hold large and diverse sets of data that are valuable as a means of improving service delivery, decision-making and policy development. Public sector organisations are subject to a range of data security legislative and policy regimes that establish obligations to both classify and protect data sets. At present, the data security settings differ between jurisdictions serving as a barrier to exchanges of large and complex data sets which could be leveraged to improve public sector performance.

Australian industry is the source of Australian wealth and prosperity and both generates and has the opportunity to leverage data sets to improve the efficiency of their operations. Australian businesses are subject to data security legislation and regulation from both the Australian Government and from the state or territory governments in which they operate. This includes legislation covering the need to protect the privacy of individuals. Some industries are subject to additional regulation in recognition of their particular role in the economy and their delivery of critical functions.

While similar data sets may be held by government, industry and individuals, the role of each within the economy warrants a different approach to the development of data security measures. This paper will look at these three groups separately as distinct actors at varying degrees of maturity and with different risk profiles.

Figure 2 – Data use has benefits for all Australians (source – Australian Data Strategy)

Improved service delivery

Data and analytics drive evidence-based decision-making and continuous refinement of government and business operations to deliver more efficient and effective services to the public and consumers.

Job creation and economic growth

Innovation data use and analytics can lead to new products, services, business models and industries, spurring jobs and economic activity.

Agility and resilience

Strong data use, sharing and management can allow government and business to quickly and flexibly identify, understand and respond to emerging issues and crises, like the impact of COVID-19.

Better outcome

Greater data use and sharing creates opportunities to reduce the regulatory and administrative burden on Australians by, for example, only requiring Australians to provide their information once or making it easier to demonstrate compliance.

In considering data security, it is vital that we strike a balance between enabling broader access to data to leverage its benefits, whilst mitigating security and other risks.

CASE STUDY

2020 ZHENHUA DATA SCRAPING

On 14 September 2020, it was reported that the collection of online personal data of 2.4 million people worldwide was conducted by the Chinese company, Zhenhua Data.

Of the 250,000 records recovered via the reported leak, there were records of 35,558 Australians uncovered – including state and federal politicians, military officers, diplomats, academics, civil servants, business executives, engineers, journalists, lawyers and accountants.

The report stated that information collected included dates of birth, addresses, marital status, photographs, political associations, relatives and social media IDs. Some information is also reported to be from confidential bank records, job applications, psychological profiles, and even the dark web, where data sets are for sale that have often been obtained via hacking.[4]

Insufficiently secured big data sets are highly attractive to cyber criminals. Big data sets containing personal information belonging to Australians are vulnerable to ransomware attacks. The Australian Cyber Security Centre reported that there was a 15 per cent increase in ransomware attacks on Australian organisations in the 12 months prior to October 2021. Because cyber attacks are on the rise, the probability of businesses suffering a data breach is increasing.

It is not just businesses or governments that are being affected. Individuals cannot readily access the information and support needed to ensure their data is secure. Personal information is being amassed at unprecedented levels due to its commercial value. Too often, this data is obtained with limited transparency over how the data is being stored, who has access to it and what it will be used for.

[4] China's 'hybrid war': Beijing's mass surveillance of Australia and the world for secrets and scandal | ABC News

Ride-share apps collection and storage of data

The ride-sharing industry is booming globally. App-based taxi services such as Uber and Lyft grew from transporting just a small number of passengers in 2012 to nearly 4 billion in 2018. Common ride-share apps collect enormous amounts of data, including ride details, address books and search history, with some apps also tracking users after they leave the car. This raises concerns about how the data is stored and managed. The most obvious concern is that hackers can gain access to it. Locally, the Office of the Australian Information Commissioner determined in 2021 that Uber interfered with the privacy of an estimated 1.2 million Australians and that they had failed to appropriately protect the personal data of Australian customers and drivers which was accessed in a 2016 cyber attack.

More serious, however, is the threat that authoritarian governments can demand access to the data to, for example, track specific citizens or groups in other countries. China's new Personal Information Protection Law poses a particular concern, as it gives the government significant power over data collected by Chinese companies.[5]

Identity crime

Identity crime is a prevalent form of criminal activity within Australia and worldwide. Identity crime, or identity theft, can occur when a cybercriminal gains access to your personal information to steal money or gain other benefits. They can create fake identity documents in your name, get loans and benefits or apply for real identity documents in your name, but with another person's photograph.

In 2018-19, the total direct cost of identity crime in Australia equalled $2.1 billion with costs to individuals of more than $500 million.

The indirect cost of identity crime in 2018-19 was estimated to add a further $1.0 billion to the $2.1 billion in direct costs bringing the total economic cost to $3.1 billion in Australia.[6]

Data security is a collective responsibility

For Australia to become a leading digital economy by 2030, the value of data must be maximised. The Intergovernmental Agreement on Data Sharing between Commonwealth and state and territory governments, signed by National Cabinet on 9 July 2021 is an important step for our digital economy. Increased data flows across jurisdictions will improve government service delivery. But it needs to be secure.

[5] How Ride-Share Apps Collect and Store Data: Uber found to have interfered with privacy | Office of the Australian Information Commissioner

[6] Statistical Reports 29: Identity crime and misuse in Australia 2019 | Australian Institute of Criminology

Data security is a collective responsibility where we, as a nation must remain joined up and connected on data security standards to minimise inconsistencies and prevent malicious actors taking advantage of jurisdictional difference. The current inconsistencies from jurisdiction to jurisdiction present a significant challenge to data sharing. This presents opportunities for adversaries and malicious actors and challenges for businesses and the community. The current discrepancies in approach can be highlighted by the COVID-19 response, particularly as it relates to the way in which each jurisdiction manages and stores COVID check-in data, including where and how it is stored. Similarly, each jurisdiction issues identity documents such as driver licences, which contain personal information, including an individual's biometrics that may be used by malicious actors.

In order to have a significant national impact and build community confidence, it is essential that a baseline is established and raised across the Federation to ensure that all Australian data is held to the same level of security regardless of the jurisdiction.

Data security by the numbers

- The global 'data sphere' continues to increase exponentially, and in the five years from 2019 to 2024 it is expected to increase from 45 zettabytes to 143 zettabytes.[7]
- The average cost of a single data breach increased globally by nearly 10 per cent year over year to $5.9 million in 2021, the highest average cost recorded and largest single year cost increase in the last seven years.[8]
- Customer personal information was the most common and most expensive type of record lost or stolen in a data breach, costing on average $252 per record.[9]
- Both system complexity and degree of compliance failures contributed to the higher cost of data breaches globally, including organisations with high compliance failures paying an average of $3.2 million more for data breaches in 2021.[10]
- Data breach costs accrue over several years. On average, 53 per cent of global data breach costs were incurred in the first year, 31 per cent in the second year, and 16 per cent more than 2 years after the event.[11]
- In 2021, the average time to identify a breach globally is 212 days, and the average time to contain it is 75 days; totalling a 287 day breach lifecycle. Meanwhile, a hacker can infiltrate an entire customer database in a matter of hours.[12]

[7] Worldwide Global DataSphere Forecast. 2021-2025: The World Keeps Creating more Data – Now, What Do We Do With It? | International Data Corporation
[8] Cost of a Data Breach Report 2021 - Australia | IBM
[9] Cost of a Data Breach Report 2021 - Australia | IBM
[10] Cost of a Data Breach Report 2021 - Australia | IBM
[11] What is the Cost of a Data Breach in 2021 report | UpGuard
[12] What is the Cost of a Data Breach in 2021 report | UpGuard

AUSTRALIA'S CURRENT DATA SECURITY LANDSCAPE

The Australian Government is progressing multiple initiatives to ensure proportionate and fit-for-purpose protections for data across the economy. These include a number of initiatives introduced to address prominent vulnerabilities, such as the current review of the *Privacy Act 1988*, amendments to the *Security of Critical Infrastructure Act 2018*, the National Ransomware Action Plan and the Hosting Certification Framework. However, it is important to recognise that these legislative and policy initiatives were developed and introduced for specific purposes, and typically revolved around a single type of information or storage concern. In addition, acknowledging that there are – appropriately – different measures and mechanisms in place to support data security for governments, industry and consumers creates a congested environment. Figure 3 below also highlights the landscape as it relates to government bodies and their connection to support domestic data security.

Figure 3 – Existing Australian Government data bodies

Entity	Role	Government mechanisms		
Office of the Australian Information Commissioner	Independent national regulator for privacy and freedom of information	🟥 *Privacy Act 1988* and the Australian Privacy Principles	🟩 Overseas data frameworks with extra-territorial application in Australia	
Attorney-General's Department	Maintain and improve Australia's law and justice framework, and facilitate jobs growth through policies that promote fair, productive, flexible and safe workplaces		🟪 Protective Security Policy Framework	🟪 General Security Agreements (GSA) and arrangements
Department of Home Affairs	Australian Government policy lead for data, cyber and critical infrastructure security	🟪 Hardening Government IT	🟥 *Security of Critical Infrastructure Act 2018*	
Australian Cyber Security Centre	Leads the Australian Government's efforts to improve cyber security		🟪 Information Security Manual	
Digital Transformation Agency	Responsible for strategic and policy leadership on whole-of-government and shared ICT investments and digital service delivery		🟪 Data Centre Facilities Supply Panel	🟪 Whole-of-government Hosting Strategy and Hosting Certification Framework
Office of the National Data Commissioner	Responsible for streamlining how public sector data is used and shared	🟪 Data Availability and Transparency Bill		
Treasury	Supports and implements policies which enable strong, sustainable economic growth and fiscal settings	🟥 Consumer Data Right	🟥 *Foreign Acquisitions and Takeovers Act 1975*	
Department of Prime Minister and Cabinet	Coordinating public data policy, and the Australian Data Strategy	🟥 Australian Data Strategy		
National Archives of Australia	Implement policy to ensure agencies property manage information assets (incl. data)	🟪 *Archives Act 1983*		

🟪 Public sector data 🟥 Public sector data, business data and personal information 🟩 Business data and personal information

UNDERSTANDING YOUR DATA SECURITY CONCERNS

This discussion paper builds on the feedback received by the Australian Government through recent consultation on complementary bodies of work, such as the *Security of Critical Infrastructure Act 2018* and Australia's Cyber Security Strategy 2020, to develop clear and consistent data security expectations.

Government, led by the Federal Government, needs to be an exemplar

- The Australian public is concerned about how the Government collects, uses and shares its data, particularly personal information such as biometrics.
- Government can do more to reinforce transparency in handling of personal information.
- Government and non-government stakeholders emphasised the need for alignment in how the Government discusses data ownership.
- Government can maintain trust that minimum standards are in place to protect data by harmonising data security laws across the jurisdictions.
- Government's role should be to protect Australians' security and privacy, and the data it holds about its citizens. Government should look to create a shared best practice community.
- Government seeks to regularly engage with industry to develop creative and technology-driven solutions that would enable a better balance between the tremendous opportunities enabled by digital platforms and the legitimate safety needs of the community.

Everyone has a role to play

- Roles and responsibilities for data security need to be clarified and rebalanced between government, industry and the community.
- Small business and local governments are particularly vulnerable to cyber security threats.
- Increasing data aggregation has significantly increased the risk of serious data breaches exposing the personal information of all Australians.
- Stakeholders generally believed that consumers and small businesses were particularly vulnerable to data breaches due to a lack of resources, capability and expertise to manage cyber security risk.
- Most stakeholders strongly supported increased adoption of secure by design principles by manufacturers and software developers to better support consumers and small businesses to strengthen their cyber security and protect their data.

LOOKING AHEAD

The National Data Security Action Plan

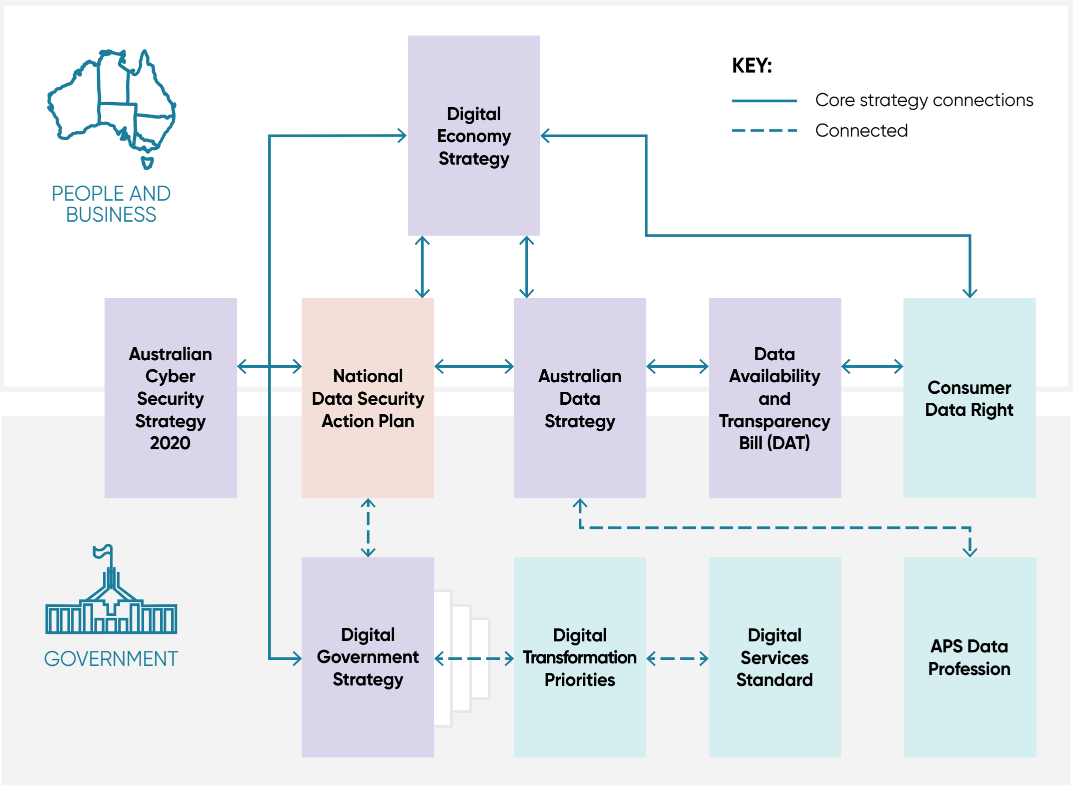
The Action Plan is a new approach for the Australian Government. It is an opportunity to develop a clear articulation of the settings and requirements for governments, businesses and individuals while ensuring consistency and driving uplift through new and complementary measures.

The Action Plan will leverage existing legislative and policy mechanisms as a means to further strengthen and coordinate Australia's data security policy settings. It will provide the Australian Government with new options to cover any existing or emerging gaps based on intelligence analysis and feedback received in response to this discussion paper, as well as previous consultations on associated measures.

The Action Plan sits alongside Australia's Cyber Security Strategy 2020 to ensure the settings are fit for purpose to support the increased connectivity and need for digital trust that comes with a digital economy. Together, the Action Plan and Cyber Security Strategy will set a strong security foundation for the Australian Data Strategy and the Digital Government Strategy as key enablers under the Digital Economy Strategy.

How these complementary strategies are connected is summarised is detailed in *Figure 4*.

Figure 4 – Complementary Australian Government Digital Strategies


PEOPLE AND BUSINESS
KEY:
Core strategy connections
Connected
Digital Economy Strategy
Australian Cyber Security Strategy 2020
National Data Security Action Plan
Australian Data Strategy
Data Availability and Transparency Bill (DAT)
Consumer Data Right
GOVERNMENT
Digital Government Strategy
Digital Transformation Priorities
Digital Services Standard
APS Data Profession

Protecting the data most critical to our way of life

Safeguarding critical infrastructure data that underpins our way of life is paramount. The digitalisation of Australian Government services will increase the Australian Government's data holdings, storage requirements and the criticality of the data underpinning these functions. As highly sophisticated state-sponsored and criminal actors continue to target governments and industry data, the security of data storage and processing assets providing critical services to Australia, and the necessity of effective control, visibility, and assurance of the security of Australian Government data is paramount. The Australian Government is taking significant steps to ensure government and critical infrastructure data is secure, building on existing mechanisms including the Protective Security Policy Framework.

These include:

- **The *Security of Critical Infrastructure Act 2018*** recognises that data storage and processing is now a critical infrastructure sector. The Act will drive data security uplift across the data storage and processing sector, as a key provider of data related services to government while also ensuring that the business critical data belonging to designated assets from the other critical infrastructure sectors is stored and processed securely.
- **The Whole-of-Government Hosting Strategy** identifies sovereign issues within hosting supply chains and the need to mitigate against supply chain and data centre ownership risks, through the implementation of a certification framework and effective governance model.
- **The Hardening Government IT** program will centralise government cyber capabilities and harden Australian Government networks at scale against the pervasive and increasing cyber security threat with a Cyber Hub pilot already underway.

The National Data Security Action Plan will assess the implementation of these initiatives as they progress and consider further options to uplift government data security.

A PRINCIPLES-BASED APPROACH TO DATA SECURITY

Introducing the data security pillars

The Australian Government has developed three core pillars that present a consistent, proportionate and scaled approach to data security across the Federal, state and territory governments and industry. These pillars will underpin the Action Plan.

Pillar	What it means
Secure	Security is knowing how well data is protected, by whom and secured to a level commensurate with the value, importance, sensitivity and volume of the data held. The Action Plan will support the Secure pillar to set consistent and mandatory data security standards and communicate advice, expectations and requirements across the economy.
Accountable	Accountability is knowing that the data is secure and custodians held accountable through clear and concise guidance, policy and legislative mechanisms to ensure that data is stored with appropriate standards. The Action Plan will support the Accountable pillar through mechanisms to support accountability, responsibility and assurance for Government and commercial data centres, and to enhance visibility of the value of data to support proportionate protection and disclosure of data.
Controlled	Control is knowing what is happening to data in transit and at rest, what data is being stored, where it is being stored, who has access to it, and having the ability to freely remove, transfer and destroy the data without consequence within existing legislative obligations. The Action Plan will support the Controlled pillar through enhancing and promoting mechanisms for individuals to control the use and collection of their data.

CALL FOR VIEWS
BUILDING A COMMON UNDERSTANDING

A combination of inconsistent definitions, misused terms and complex data guidance create confusion and uncertainty for government, industry and individuals. Agreeing on key data security terms and concepts is fundamental to addressing confusion, misunderstandings and establishing clarity for the whole economy.

What do we mean by data?

Data is any information in a form capable of being communicated, analysed or processed (whether by an individual or by computer or other automated means).[13]

Government and industry may have differing definitions of data depending on the aims, context or use of the data. Data may comprise both paper and digital records about different types of information. As an asset underpinning nearly every aspect of the digital economy, data regulation and guidance is currently captured through a variety of different sectoral and thematic channels.

Some existing mechanisms, for instance, may specifically capture particular subsets of data or sensitivities—such as business critical data through the amended *Security of Critical Infrastructure Act 2018* or personal information under the *Privacy Act 1988* (the Privacy Act) and the current review of that Act being undertaken by the Attorney-General's Department.

What is data security?

Data security refers to protecting the information collected, processed, and stored on digital systems and networks.[14]

[13] Consistent with the Australian Data Strategy and the Data Availability and Transparency Bill
[14] Consistent with the Australian Cyber Security Centre's definition of data security

This is distinct to the related concept of cyber security, which encompasses measures to protect the confidentiality, integrity, and availability of systems, devices, and the information residing on them.

International obligations

Nations around the world are actively seeking to ensure the data that is most valuable to their national security and economic prosperity is protected and secured. Domestic data security laws and obligations vary greatly from country to country. Australia seeks to promote strong and ethical data security standards that promote cross-border data flows, support human rights, digital trade and public trust in the protection of datasets.

Cross-border data flows

International data flows are critical to today's diversified value and supply chains as they enable global e-commerce and underpin contemporary cloud computing services where servers are dispersed across multiple countries to improve access speed and optimise network traffic. International data flows are necessary for consumer-to-consumer interactions, and it is estimated that they will add $15.4 trillion to the global economy by 2025[15]. International data flows have also been crucial throughout the COVID-19 pandemic in enabling the rapid sharing of research data and pooling resources to understand the virus and develop better diagnostics, therapies and vaccines.

International flows of finance and investment have enabled rapid development for smaller economies in the modern global economy. Foreign investment into Australia helps finance new industries and enhance existing industries, boosting infrastructure and productivity and creating employment opportunities.[16] International capital flows are also vital for digital transformation. Emerging technologies such as AI are reliant on large amounts of data to train and develop AI tools. Often, the data required to unlock these benefits resides in other jurisdictions, both across domestic governments and overseas.

Digital trade rules

To enable and maximise the benefits of cross-border data flow, there is a need to include balanced trade rules that push back against unnecessary restrictions on the flow of data across borders and on where data is stored, with strong privacy, data and consumer protections. Protectionist digital measures are on the rise in our region. Governments are increasingly establishing barriers to digital trade such as measures to prevent the free flow of data and requirements to use domestic computing facilities for protectionist and authoritarian purposes. Australia recognises that government and industry have mutual responsibilities and interests in maximising the opportunities and mitigating the risks of cross-border data flows.

[15] Regulating for a digital economy: Understanding the importance of cross-border data flows in Asia | Meltzer & Lovelock

[16] The benefits of foreign investment | Department of Foreign Affairs and Trade

Despite the clear potential benefit of cross-border data flows, countries can be fragmented in their approach to data regulation. To reduce digital trade barriers, Australia has agreed with a number of countries to avoid certain data localisation laws. For example, the Australia-Singapore Digital Economy Agreement prevents unnecessary restrictions on the transfer and location of data between Singapore and Australia, while preserving the ability to implement certain measures achieving legitimate public policy objectives. This supports businesses operating in both countries by encouraging innovation in their products and services, thereby increasing competitiveness in local and international markets.

Further abroad, bilateral or multilateral agreements govern international data flows, such as the European Union's General Data Protection Regulation or United States-Mexico-Canada Agreement. This fragmented approach to data regulation highlighted above can prohibit or significantly encumber the free flow of data due to varied privacy, security and data access legislation and policies. The result is a global data governance landscape that selectively restricts the free flow of data and sets uneven data handling and storage requirements.

Data localisation – Getting the balance right

Local storage requirements can protect sensitive information or information which may pose national security threats if transferred overseas. However, local storage of data has nuanced security implications and cannot in itself guarantee security. Many countries have data localisation laws in place, while others are adopting legislation, often to stop insecure transfer of personal information across borders.

While data localisation laws may be justified in some instances, widespread local storage requirements can represent significant barriers to trade and economic cost. Some of Australia's legislation prohibits or restricts the storage, processing and transferring of particular data overseas. Data localisation measures within Australian Commonwealth legislation seek to ensure that operating entities can be audited for financial compliance; overseas disruptions do not affect the continued operation of Australian financial systems; and the security of particular subsets of personal and sensitive information is protected. For example, Commonwealth legislation prevents registered operators and service providers from storing, transferring, processing or handling My Health Record information offshore.

Australia is a trusted and influential partner in the international community. Australia seeks to contribute to priority initiatives such as international data standards, and data flows that are safe, secure, lawful and ethical and in line with Australia's values and interests. We also seek to balance international data sharing obligations with proportionate protections to ensure the security of Australian information, such as sensitive national security information.

What can you provide?

Data service providers often have global footprints, and may be subject to a variety of data security obligations and practices across the relevant jurisdictions. Additionally, restrictive local data security obligations can affect an entity's ability to engage internationally and drive innovation.

Government is seeking views on how it can proportionately uplift protections for personal information of Australian citizens, while balancing the opportunities presented by international data flows and the global economy.

Call for views:

1. What do you consider are some of the international barriers to data security uplift?
2. 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)?
3. What additional guidance or support from Government would assist you to meet a principles-informed approach to data security? How would this be delivered best to you?
4. 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?
5. Does Australia need an explicit approach to data localisation?

GOVERNMENT'S ROLE – FEDERAL, STATE AND TERRITORY AND MUNICIPAL GOVERNMENT UPLIFT

State, territory, and municipal governments generate large sets of data that are valuable as a tool for policy development, service delivery and government decision-making. For these same reasons, it is also highly attractive to foreign adversaries and malicious actors.

The increasing complexity of policy challenges beyond jurisdictions warrants a coordinated approach founded upon a common set of security standards that maximises trust and enables practical and efficient collaboration. At present, the Commonwealth and each State and Territory Government, has their own security classification system, and as such, similar data sets may be classified (and protected) differently between jurisdictions. In addition, privacy legislation is similar but not entirely harmonised across the states and territories and not all states and territories have their own privacy laws. This presents inconsistent standards for protection of personal information across different levels of government.

The harmonisation and enhancement of data security standards across all jurisdictions will ensure public trust in the handling of personal and sensitive information is maintained to enable the growth in digital government services. We welcome suggestions on how to best develop a harmonised approach and avoid siloed data security policy arrangements between jurisdictions.

Call for views

6. How can data security policy be better harmonised across all jurisdictions? What are the key differences between jurisdictions that would impact the ability to implement standardised policies/are there any areas of policy that could not be standardised? If yes, why?
7. Who is currently responsible for ensuring consistent and commensurate uplift of local government data security and how can this be strengthened? Do you think responsibilities should be shared across more bodies, or shifted elsewhere entirely?
8. What are the main challenges currently faced by industry as a result of inconsistent data security practices between all levels of Government, including municipal governments?

CLARITY AND EMPOWERMENT FOR BUSINESS

Businesses generate and process multitudes of data, including personal information of consumers and data used for business operation. Large corporations are no longer the only entities holding large and sensitive data sets. Small and medium-sized businesses, due to the increase of digital commerce, are collecting an increasing amount of personal and sensitive information. Small and medium-sized businesses are traditionally less equipped in securing data, and are often the victims of data breaches and ransomware attacks.

A data set is of equal intrinsic value regardless of whether it is held by a private sector organisation, a private individual, or a government entity. However, government entities are subject to additional legislative regulatory and administrative policy standards that do not apply to private sector organisations (unless the organisation is contracted to hold the information for a public sector entity). As such, private sector security standards and controls can vary between organisations. While it is appropriate to seek to minimise regulatory burden, consideration needs to be given to how Australian data held by the private sector can be appropriately protected.

The Australian Government is committed to supporting small and medium businesses, along with larger industry players to raise awareness and uplift data security posture across all sectors.

Data security guidance for industry currently varies depending on size, sector and type of data. These include:

- the *Security of Critical Infrastructure Act 2018*
- the *Privacy Act 1988* and the Australian Privacy Principles (small businesses are exempt from the Act, but may otherwise benefit from this guidance as best practice)
- cyber.gov.au
- the Consumer Data Right, established under the *Competition and Consumer Act 2010.*

A key factor in appropriately securing data is understanding the value and risk connected to the data in isolation and aggregated form. We seek feedback on how to improve guidance for businesses at all levels on how to secure data according to its sensitivity and vulnerability to malicious actors. We welcome suggestions on how to raise awareness to businesses on data security practices, especially those not captured under the Privacy Act and the Critical Infrastructure and Systems of National Significance regulatory reforms.

Data centres

Both government and the private sector have gravitated towards using large data centres, leading to a concentration of data storage. Co-location arrangements can create economies of scale for the development of sophisticated and layered security measures while providing a smaller threat surface. However, significant use of a single supplier heightens data aggregation-related risk and reduces the redundancy that comes with diversity. Over-concentration without adequate redundancy risks creating single points of vulnerability, whereby a failure or a compromise could disable entire functions or services. We welcome views on how effective the current settings are, including the recent introduction of the Hosting Certification Framework, at strengthening diversity within the market without diminishing security outcomes.

Supply chains

Third party providers can introduce additional vulnerabilities into an entity's supply chain, including through a weak data security posture. Current advice includes the Australian Government's Critical Technology Supply Chain Principles (the Supply Chain Principles), which assist businesses in making decisions about their suppliers and technology solutions.

The Supply Chain Principles are grouped under the three pillars: security-by-design; transparency; and autonomy and integrity. Having a clear understanding of where your technology comes from will help you to understand where there may be vulnerabilities in your technology supply chain, and what steps you can take to secure your data.

Call for views

9. What steps could your business take to better understand the value of the data they process and store? Do businesses have sufficient awareness of their data security obligations?
10. How can the Australian Government further support your business to understand the value of data and uplift your data security posture?
11. Does your business appropriately consider data security risks in their supply chains? Is there sufficient public information provided by Government to help your business identify these risks?
12. Should there be overarching guidance on securing data for businesses of all sizes, or is it important to provide guidance based on a company's size? For example, a 'size' threshold).
13. Are there any limiting factors that would prevent Australian industry and businesses from effectively implementing an enhanced data security regime?

EMPOWERING AND EDUCATING CITIZENS AND CONSUMERS (THE COMMUNITY)

Citizens and consumers generate and provide an increasing amount of data to governments and businesses, often in exchange for a good or service. With the massive growth in the digital economy, especially due to the COVID-19 pandemic, personal information is more frequently exchanged. This includes biometric data used for face recognition to verify a person's identity. With the increased digitisation of service delivery and the broader economy, it is sometimes not possible for consumers to know where their personal information is, or who has access to it. While the free-flow of data enables the digital economy, data security is equally as important to ensure digital identities and sensitive information are protected.

Citizens' and consumer personal information is protected through the Privacy Act. The Privacy Act promotes and protects the privacy of individuals and regulates how certain Australian Government agencies and organisations handle personal information. The Privacy Act is undergoing a review that seeks to ensure privacy settings empower consumers, protect their data and best serve the Australian economy. The Attorney-General's Department is also progressing the introduction of an Online Privacy Code, which will strengthen privacy protections for individuals using social media and certain other online platforms, as well as increase penalties and other enforcement measures for the Office of the Australian Information Commissioner.

The National Data Security Action Plan will assess the implementation of these initiatives as they progress and consider further options to uplift government data security.

The Australian Government has existing published guidance for various data security related issues through the:

- Australian Cyber Security Centre
- e-Safety Commissioner
- Office of the Australian Information Commissioner
- Office of the National Data Commissioner.

These platforms provide tailored advice to individuals and vulnerable members of society in navigating the complex digital landscape, including securing their personal information.

We welcome views from the public on how the Government can better adapt our approach to ensure there is a common understanding of data security in the community.

Call for views

14. Does the Australian Government currently have sufficient public information for consumers and citizens on data security best practice? How can we make that information more easily accessible, usable and understandable?
15. Should there be enhanced accountability mechanisms for government agencies and industry in the event of data breaches? How else could governments and industry improve public trust?

NEXT STEPS

To ensure an appropriate co-design process, we welcome feedback on any additional data security policy issues not addressed in this discussion paper or any other issue relating to data security that Government should consider.

These can provided at: https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/data-security.

CALL FOR VIEWS

1. What do you consider are some of the international barriers to data security uplift?
2. 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)?
3. What additional guidance or support from Government would assist you to meet a principles-informed approach to data security? How would this be delivered best to you?
4. 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?
5. Does Australia need an explicit approach to data localisation?
6. How can data security policy be better harmonised across all jurisdictions? What are the key differences between jurisdictions that would impact the ability to implement standardised policies/are there any areas of policy that could not be standardised? If yes, why?
7. Who is currently responsible for ensuring consistent and commensurate uplift of local government data security and how can this be strengthened? Do you think responsibilities should be shared across more bodies, or shifted elsewhere entirely?
8. What are the main challenges currently faced by industry as a result of inconsistent data security practices between all levels of Government, including municipal governments?

9. What steps could your business take to better understand the value of the data they process and store? Do businesses have sufficient awareness of their data security obligations?
10. How can the Australian Government further support your business to understand the value of data and uplift your data security posture?
11. Does your business appropriately consider data security risks in their supply chains? Is there sufficient public information provided by Government to help your business identify these risks?
12. Should there be overarching guidance on securing data for businesses of all sizes, or is it important to provide guidance based on a company's size? For example, a 'size' threshold).
13. Are there any limiting factors that would prevent Australian industry and businesses from effectively implementing an enhanced data security regime?
14. Does the Australian Government currently have sufficient public information for consumers and citizens on data security best practice? How can we make that information more easily accessible, usable and understandable?
15. Should there be enhanced accountability mechanisms for government agencies and industry in the event of data breaches? How else could governments and industry improve public trust?

Australian Government