February 2025

## UPDATE

# Recap on law made late 2024

Did you come back from holidays trying to remember what the happened at the end of 2024 and what you might need to do about it?

In this start of year recap, we briefly summarize the significant tech related Australian regulatory changes made late 2024 and suggest some possible responses.

| | **Legislative Change** | **Actions to consider** |
|---|---|---|
| 1. | *Cyber Security Act 2024* introduced<br>• a framework for the issue of **mandatory security standards** for certain products that can connect to the internet.<br>• **Mandatory ransom payment reporting** for entities that make ransomware payments. Bodies must report to a designated Commonwealth body within 72 hours.<br>• a **National Cyber Security Coordinator** tasked with leading the whole-of-government coordination and triaging of action in response to significant cyber security incidents. A framework to facilitate voluntary information sharing with the Coordinator in relation to significant cyber security incidents. The coordinator is also able to direct impacted entities to other services that may assist them.<br>• a **Cyber Incident Review Board** that will conduct reviews of significant cyber security incident, make recommendations to government and industry about actions to prevent, detect, respond to, or minimise the impact of incidents in the future and request and compel information from entities involved in cyber security incidents under review.<br>• a framework for sharing of information about cyber security incidents with government entities. | If you have products that could be subject to the proposed mandatory standard for connected devices:<br>• monitor and perhaps input into the standards development process.<br>• Consider whether certification will influence your purchasing decisions.<br>• Develop and implement compliance.<br>Develop internal procedures and systems to ensure compliance with the ransomware payment reporting obligations.<br>Consider the benefits of engaging with the National Cyber Security Coordinator. Including understanding the Coordinator's role in responding to significant cyber incidents and when you may provide information voluntarily.<br>Consider the implications of the Cyber Incident Review Board's powers to compel information, and that the Board can review significant cyber security incidents.<br>Consider updating security policies accordingly. |

| | | |
|---|---|---|
| 2. | *Digital ID Act 2024* introduced*:*<br>• an **Accreditation Scheme** for entities as attribute service providers, identity exchange providers, identity service providers, or other prescribed service providers. Accreditation is voluntary but required for participation in the A**ustralian Government Digital ID System (AGDIS)**<br>• an expansion of the AGDIS for use by Commonwealth, State, and Territory governments as well as the private sector.<br>• **Digital ID Data Standards Chair** who makes Digital ID Data Standards and reviews them regularly.<br>• requirements for record keeping by participating entities and the destruction or de-identification of certain information. | The use of the digital identity system may be an opportunity to improve efficiency and reduce privacy risk by avoiding the need to collect and hold identification records. Investigate becoming an accredited entity under the Act.<br>Once in operation for private entities, assess the relative cost and complexity of participation compared to the maintenance of existing authentication arrangements. |
| 3. | *Intelligence Services and Other Legislation Amendment (Cyber Security) Act 2024* introduced:<br>• a **'limited use' obligation** for the Australian Signals Directorate (ASD) regarding cyber security information that is voluntarily provided to them, or which they have acquired or prepared, meaning it can only be used for specified cyber security purposes:<br>o The Act defines **'limited cyber security information'** as data relating to a cyber security incident that has occurred, is occurring, or may potentially occur. This includes information shared by impacted entities or acquired by ASD with consent. It also includes vulnerability information.<br>o ASD can share limited cyber security information, including aiding incident response, informing ministers, and collaborating with other Commonwealth and State bodies, as well as intelligence | Consider implications of the scope of "limited cyber security information".<br>Consider benefits of increased information sharing with the ASD:<br>Consider updating risk management policies to incorporate sharing with ASD. |

| | | |
|---|---|---|
| | agencies and the Inspector-General of Intelligence and Security<br>• limits to the use of shared information in civil or regulatory actions, except for criminal offences. The Act also restricts the **admissibility of this information in court** and prevents ASD staff from being compelled to testify about it. | |
| 4. | *Privacy and Other Legislation Amendment Act 2024* introduced:<br>• a requirement to include information in their privacy policies about the types of personal information used in computer programs that make decisions (**automated decision making**) that could significantly affect an individual's rights or interests.<br>• an obligation to maintain Security measures that include "technical and organisational measures".<br>• potential legal **action for serious invasions of privacy** . This new statutory tort covers both intrusion upon seclusion and misuse of personal information.<br>• a requirement that the Privacy Commissioner develop a **Children Online Privacy Cod**e within 24 months. The Minister can specify the matters the code must address and the entities that must comply with it. The Minister can direct the Commissioner to develop temporary code which can be in force for up to 12 months and are not subject to disallowance.<br>• a broader range of **enforcement options**, including new civil penalty provisions, and the power to issue compliance notices, to conduct public inquiries into specified matters related to privacy and the ability to issue infringement notices for minor breaches of the Privacy Act.<br>• new criminal offences address **doxxing,** the malicious exposure of an individual's personal data online. | **Regulated e**ntities must review and update their privacy policies to:<br>• Identify and make the required disclosures regarding automated decision making.<br>• Ensure that data security measures cover technical and organisational measures.<br>• When made, comply with the Children's Online Privacy Code.<br>Regulated entities may consider:<br>• risk mitigation strategies to avoid engaging in a serious invasion of privacy, suffering compliance notices and/or penalties and/or the use of Ministerial information sharing powers.<br>• updating policies and procedures and undertaking internal training to support compliance.<br>• protocols for sharing personal information during declared emergencies or data breaches, in compliance with the new provisions. |

| | | |
|---|---|---|
| | • powers for the Minister to make declarations that allow entities to handle personal information in ways not usually permitted under the Australian Privacy Principles (**APPs**) to prevent or reduce the risk of harm following an eligible data breach . | |
| 5. | *Security of Critical infrastructure and other Legislation Amendment Act 2024* introduced*:*<br><br>• a definition of critical infrastructure assets expanded to include **data storage systems** that hold "business critical data" and are related to the functioning of a primary asset.<br>• government **powers to respond any incident**, including those caused by natural disasters or physical attacks, that could impact the availability, integrity, or reliability of critical infrastructure.<br>• **written directions** to entities to address any serious deficiencies in their critical infrastructure risk management programs.<br>• consolidated **security requirements for critical telecommunications assets**.<br>• a revised, harms-based definition of '**protected information**' and revised disclosure provisions to enable more effective and timely sharing of information.<br>• Removal of:<br>  ○ the requirement for the Minister to notify direct interest holders of a declaration of an asset as a System of National Significance (**SoNS**).<br>  ○ the obligation for responsible entities to advise the Secretary of all instances when direct interest holders change for a given asset.<br>• power for the Secretary of the Department of Home Affairs, when authorised by the Minister, may issue directions as a 'last resort' to manage | Regulated entities must review and update their Critical Infrastructure Risk Management Programs (**CIRMP**) to incorporate the expanded definition of critical infrastructure assets including:<br><br>• ensuring that data storage systems holding 'business critical data' are considered within their risk assessments.<br>• identifying and implementing controls to mitigate or eliminate risks to these data storage assets, as part of their CIRMP obligations.<br>• Entities should proactively identify and control against risks to their data storage assets.<br><br>Consider the implications of and revise policies to account for the:<br><br>• New scope of protected information and what this means for the handling of information related to relevant critical infrastructure assets<br>• New powers that allow the regulator to issue directions to vary their CIRMP.<br>• possible directions to address the consequences of significant incidents.<br><br>Entities responsible for a critical telecommunications asset, must be aware of the new security obligations transferred from the Telco Act to the SOCI Act. |

| | | |
|---|---|---|
| | the consequences of serious incidents impacting critical infrastructure asset. | |
| 6. | *Telecommunications Amendment (SMS Sender ID Register) Bill 2024* introduced:<br>• an obligation for the Australian Communications and Media Authority (ACMA) to establish and maintain an **SMS Sender ID Register**.<br>  ○ The SMS Sender ID Register will contain sender identifications accepted by the ACMA, and other kinds of information.<br>  ○ The purpose of the register is to reduce SMS scams by allowing legitimate entities to register their sender identifications.<br>• power to refuse or revoke approvals to register and can remove entries from the register if a sender ID is offensive, misleading, deceptive, or a spoofing sender identification.<br>• power for ACMA to make determinations, by legislative instrument, relating to applications for registration, access to the register and its administration and operation. | Organisations that use SMS for marketing and customer communications may wish to:<br>• monitor the development of the register and the processes that support it.<br>• respond to any consultation undertaken by ACMA.<br>• in due course, consider an application for approval to register, register of sender identification.<br>• stay informed about relevant ACMA determinations.<br>Monitor for a decision regarding whether the register will be voluntary or mandatory. Monitor the creation of binding standards setting the detail of the scheme. These standards could require registration in order to send SMS messages to Australian mobile phones.<br>Entities may also be required to send messages with a warning tag if they are not registered or if you are not the registered party. |

## Updated Chart of Australian National Security Agencies available for download

On 28 July 2024 the Prime Minister announced that responsibility for ASIO was being moved from the Home Affairs portfolio to the Attorney-General. An updated version of the PFA chart of National Security Agencies is available for download here.

**Please contact me if you have any questions regarding the matters discussed in this update. patrick@patrickfair.com 0411361534**

**You can subscribe to updates like this one at www.patrickfair.com**