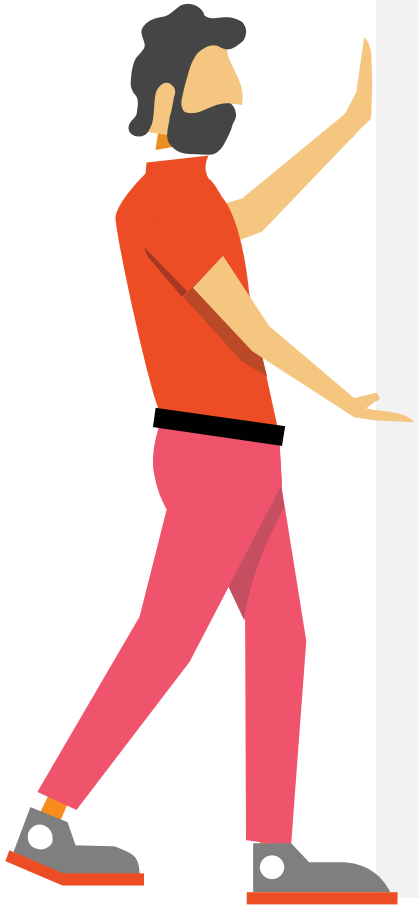
2020 Australian Privacy Outlook

PwC Legal
April 2020

Content



A new cyber and privacy focused agenda

This second edition of the Privacy Outlook provides a summary of the key privacy issues and regulatory trends impacting privacy and cybersecurity in Australia in 2020.

2020 was expected to be a year for further developments in the strengthening of privacy and data related laws in Australia. Significant events resulting in business disruption across the economy have created an even greater focus in this regulatory environment, highlighting the need for greater robustness of cyber security and privacy frameworks at a time of heightened vulnerability and greater awareness of cyber scams. For example, the COVID-19 pandemic has resulted in significant increase in the collection, use and disclosure of personal health information by government and private organisations in Australia and around the globe. Given the increased possibility of being targeted by cyber criminals in the current environment, it is imperative that organisations understand their data security and data breach notification obligations and act quickly in the event of a breach.

The focus on privacy has been front of mind for many organisations following the Australian Government's announcement that it was looking to reform the *Privacy Act 1988* (Cth) (Privacy Act) prior to the last election, together with its response to the Australian Competition and Consumer Commission's (ACCC) Digital Platforms Inquiry Report calling for a full review of the Privacy Act. In addition, the ACCC has had continued involvement in data-related practices such as the consumer data right (CDR), the use of data by digital platforms and customer loyalty schemes, and with the intersection of privacy with the Australian Consumer Law through the ACCC's Federal Court of Australia action against Google.

Recent recommendations have been made for an increase of the powers and resources of the Office of the Australian Information Commission (OAIC), which could lead to greater investigation and enforcement activity by the OAIC, as well as for increased penalties for breaches of the Privacy Act to match those associated with breaches of the Australian Consumer Law.

It is expected that developments in AI and technology will result in an increased need for stronger measures to be implemented, such as an AI ethical framework, a better understanding of the Assistance and Access Bill and data sharing between governments.

This paper highlights some of the key areas of regulatory change on the horizon for cyber and privacy.

Business disruption, cybersecurity and privacy compliance

Recent disruptive events (such as the COVID-19 virus pandemic) have increased the need for the implementation of robust cyber security measures by organisations at a time of heightened vulnerability, greater awareness of cyber scams and increases in the collection, use and disclosure of personal health information in Australia and globally.

Cybersecurity during disruption

Disruptive events often require businesses to undergo rapid changes to their operations and cyber criminals are alive to this. These threat actors will often look for opportunities to exploit as businesses move to alternative working practices, remote access, and online collaborative tools for their staff to continue doing business. Businesses should not only assess cyber risks and respond to new developments in this volatile environment to ensure business continuity, but should also be ensuring ongoing compliance with security and privacy regulations in the Privacy Act, including in relation to data breaches.

Culture and awareness

End user behaviour and culture awareness during a time of heightened cyber risk

Governance

Operating effective security governance and ensuring that existing governance structures are sufficient in the new environment

Data security

Protecting sensitive information whilst implementing and operating different working practices

Capacity management

Managing increased demand on the critical security services needed to enable remote working and secure data access

Detective/protective controls

Maintaining effective monitoring, detection and protection controls during non-standard business operation

Incident management and business continuity

Continuing to operate incident management, crisis response and business continuity capabilities during a period of increased organisational stress

Business disruption and privacy compliance (cont'd)

Case study: COVID-19 Pandemic

All aspects of modern life have suffered significant disruption as a result of the COVID-19 outbreak, and the business world is no exception.

In Australia, the OAIC has published the "**Coronavirus: Understanding your privacy obligations to your staff**" Guideline to help organisations understand their privacy obligations. It is important for employers to balance their obligations of maintaining a safe workplace for staff and visitors with the appropriate handling of personal information. In addition to ensuring reasonable steps are taken to secure personal information under the Privacy Act, the OAIC has flagged some key items for businesses to consider, including:

- ✓ **'Need to know' basis** - using and disclosing personal information (including sensitive information) on a 'need to know' basis only. For example, ensuring only those in your business that 'need to know' are made aware of an employee who may have tested positive for COVID-19 (i.e. if they had been in contact with the person).

- ✓ **Only collect the information you need** – businesses should only collect what is reasonably necessary (including health information) from staff and visitors to prevent or manage COVID-19. For example, details of whether an individual has recently travelled overseas and to which countries.

- ✓ **Be transparent** - notify staff of how their personal information will be handled in responding to any potential or confirmed case of COVID-19 in the workplace.

Importantly, businesses should take great care when looking to rely on the employee records exemption under the Privacy Act in relation to health information collected about its employees when using and storing the health information, as well as quickly addressing any data breach relating to such information. Remember, only the organisation that directly employs the employees may rely on the exemption, not other corporate group members. Given the complex corporate structures that many organisations operate in, it is often difficult to establish that the entity collecting, storing and using the relevant information is also the employing entity.

Some key tips for managing and addressing the increased cyber and privacy risks posed during the pandemic lockdown are as follows:

- ✓ **Ensure your IT infrastructure and remote access capabilities are secure and fit for purpose for your workforce**. In particular, ensuring the VPN has ample bandwidth is a crucial step to avoid people abandoning this security step and sending potentially sensitive information through unsecure home networks, personal email accounts, or non-sanctioned devices.

- ✓ **Sense check your organisations' security landscape and governance structures**. It may be possible to divert some of your IT staff to more urgent security needs and review back up plans for single points of failure -- people, processes or technology. Reviewing who has access to what (and whether they need it), as well as mapping the security architecture to identify operational gaps, are all tactical steps to help your organisation adapt where needed, in times where resources may be more stretched. Further, review your governance structures, including any policies and procedures, that relate to cyber security and data protection (i.e. data breach response plans) to ensure they are sufficient in the current environment.

- ✓ **Communicate effectively and regularly with your workforce** regarding the increased threats and the need to remain vigilant in a time when they are distracted, stressed and adapting to change. This includes encouraging staff to restart their laptops or update their systems on a regular basis to ensure the latest security updates are installed.

- ✓ **Monitor your network traffic for suspicious activities around the clock.** As people may be working more flexibly (beyond the standard 9am to 5pm), cyber security teams, both internal and external, should be monitoring around the clock to detect and address anomalies as early as possible.

ACCC Digital Platforms Inquiry – Privacy Impacts

The ACCC's report from the Digital Platforms Inquiry included recommendations to review and strengthen Australia's Privacy Act, which extends beyond the ACCC's usual regulatory remit. This key recommendation has been supported by the Australian Government and will likely see a significant change to the privacy landscape in Australia.

The ACCC's Digital Platform Inquiry

Data is the 'new oil' of our global economy according to The Economist and many organisations are only now beginning to discover the true value of data that they have collected and hold through their business operations.

As they look to capitalise on the hidden commercial potential of those datasets, organisations are grappling with developing strategies for commercialisation that maintain compliance with relevant laws.

Ultimately, whilst the commoditisation of data can enhance market efficiencies, it can also encroach on an individual's privacy rights.

In this vein, in December 2019, the Australian government responded to the ACCC's Digital Platforms Inquiry dated 26 July 2019 (DPI) which provided recommendations relating to privacy law reform, competition and the regulation of the media industry. Of the 26 recommendations made by the ACCC, the government adopted seven, principally adopted 11, noted six and rejected two. The government largely supported the privacy related recommendations.

The government is taking immediate action on addressing competition concerns and will provide funding for the implementation of a sub-branch within the ACCC to monitor and investigate anti-competitive conduct occurring in the online market. However, the ACCC's recommendations regarding privacy reform have been subject to a longer timeframe.

The amendments that will flow from the DPI are significant and companies should prepare to embrace any changes to privacy laws, as it is possible that they will need to implement a refreshed compliance regime to accord with such amendments.

Government to conduct full scale review of the Privacy Act

During 2020, the government will commence a thorough review of the *Privacy Act 1988* (Cth) and consult on how best to protect consumers' privacy whilst ensuring Australia's privacy regime operates effectively.

Online services such as Google and Facebook are provided to consumers for 'free' in exchange for their personal information. These companies use consumers information for bid-advertising purposes which is a key part of their revenue generation. Whilst many consumers are relatively aware of this, they are not fully informed of the scope, and control over, personal information collected by these platforms. Because of this, it's expected that progress towards implementation of the Social Media Privacy Reforms that were initially announced in March 2019 will be seen in the coming months.

Key areas for review and consultation will include:

- the definition of 'personal information' to capture technical data and other online identifiers under the Privacy Act. This includes location data, IP address, device identifiers;
- strengthening notification requirements to ensure transparency over how data is collected and shared (with a focus on social media and online platforms initially but with the potential for similar measures to be extended to other industries;
- increasing consent requirements;
- increasing penalties for breach; and
- a wider review and reform of the Privacy Act to consider empowering consumers, including considering the rights to erasure and the creation of a statutory tort for serious invasions of privacy.

Cybersecurity trends

Cybersecurity increasingly on the minds of global business leaders

A constantly changing regulatory landscape and a spate of recent 'high profile' data security breaches is keeping many business leaders awake at night, particularly with the large fines that have been issued overseas.

PwC's 23rd Annual Global CEO Survey has identified 'over-regulation' and 'cyber-threats' as the greatest and fourth greatest threat (respectively) to their organisations growth prospects, with 33% of all respondents noting that they were 'extremely concerned' about 'cyber threats'.

Information security requirements: CPS 234

Over the last 12 months there has been a number of regulatory measures put in place to combat the threat of cyber attacks and increase the level of transparency/reporting requirements for organisations at the industry level.

Relevant to Australian Prudential Regulation Agency (APRA) regulated entities (i.e. in the finance sector) was the introduction of APRA's new prudential standard, CPS 234 Information Security which took effect from 1 July 2019.

Broadly, CPS 234 requires these entities to clearly define information-security related roles and responsibilities, maintain an information security capability commensurate with the size and extent of threats to their information assets, implement controls to protect information assets, undertake regular testing and assurance of the effectiveness of controls and promptly notify APRA of material information security incidents.

Given that the impending deadline on the transitional period for information assets managed by third parties is due to expire on 1 July 2020, regulated entities all across the country have been grappling with the challenge of imposing these obligations across their supply chains to ensure compliance.

In response to the current disruption in the economy due to the COVID-19 pandemic, APRA has signalled that it is willing to grant a 6 month extension to the 1 July 2020 date on a case-by-case basis upon application. Any applicant will need to advise APRA of the nature of its third-party arrangements, and how it is monitoring the risks associated with these arrangements, particularly given increased cybersecurity vulnerability due to the effects of the pandemic on organisations.

Notifiable data breach regime

The notifiable data breach regime (NDB regime) has now been in effect for just over 2 years. In circumstances where organisations suspect a 'breach' (i.e. loss of, unauthorised access to, or unauthorised disclosure of personal information), the NDB regime requires these organisations to carry out a reasonable and expeditious assessment of whether there are reasonable grounds to believe that the relevant circumstances amount to an 'eligible data breach'. If it is assessed that the breach is likely to result in serious harm to any of the individuals to whom the information relates, the entity must notify the affected individuals and the OAIC.

The OAIC released a 12 month insights report in the middle of 2019 and reported that it had received a total of 964 breach notifications in the first 12 months after the introduction of the regime. Of those breaches, 60% were 'malicious' or 'criminal' attacks with 35% attributed to human error. Interestingly, in the subsequent 6 month report covering the period 1 July 2019 to 31 December 2019, the OAIC reported 537 breach notifications (up 19%) with a small drop in incidents attributable to human error (around 32%).

Key takeaways

Organisations across the board need to be aware of the legal requirements associated with cyber incidents and data breach responses, and have a tried and tested response plan in place. These can exist at a national, state (i.e. health record and information regulations) and industry level.

Breach notifications to the OAIC appear to be increasing. This could be as a result of increased tendency to notify as more and more organisations see the potential ramifications of non compliance overseas or as a result of an increased frequency of attacks.

Whilst there has been a small decrease in the number of incidents caused by human error, it remains a significant portion of the incidents notified to the OAIC. Organisations should continue to provide employees with high quality training to encourage greater care/awareness when it comes to handling personal information to avoid these situations.

Consumer data right

The consumer data right

The *Treasury Laws Amendment (Consumer Data Right) Act 2019* which sets out the legislative framework for the consumer data rights regime (**CDR**) for designated sectors was passed in August 2019. The CDR creates a data-transfer and access regime, giving consumers access, and the ability to request access for other organisations, to data relating to the individual that is held by businesses and aims to improve competitive dynamics in key industries. The banking industry is the first sector to be bound by the regime, with the energy and telecommunications sectors to follow respectively.

Open banking

The *Competition and Consumer (Consumer Data Right) Rules 2020* (**CDR Banking Rules**) came into force on 6 February 2020. The CDR Banking Rules initially apply to the big four Banks, with smaller institutions to be bound incrementally. Consumers will be able to instruct their bank to provide access to data relating to their credit and debit cards, deposit and transaction accounts, as well as data relating to their mortgages and personal loans. This will facilitate an 'open banking' regime that gives consumers greater control over their spending behaviours and increased confidence in the banking industry.

The economy wide model

Importantly, each set of consumer data rules that bind designated sectors will operate under a different model. Adopting sector-specific models accommodates the functional dynamics and complexities of each industry and will enhance market efficiency. The *Consumer Data Right (Banking) Rules* will operate under an 'Economy-Wide Model'. This means financial institutions are responsible for providing the consumer's data directly to an 'accredited data recipient' (**ADR**) who then forwards this data onto the consumer.

The banking sector can leverage online banking and existing consent mechanisms already instilled in the four major banks' systems, which means some current systems may not need to change significantly. An ADR may seek access to data so long as it is willing to share 'equivalent' data in return. This principle of reciprocity will compel competitors to develop innovative services, rather than rely on the monopolistic hoarding of data. Although, this concept of reciprocity is expected to be industry-agnostic and its exact application is yet to be settled.

Key dates	
6 February 2020	CDR Banking Rules apply only to ANZ, CBA, NAB and Westpac. These banks are required to share product reference data with ADRs.
1 July 2020	Consumers will be able to request the big four banks to share their credit, debit and transaction data with service providers.
After July 2020	Consumer data rules will be enacted for the energy sector.
1 November 2020	Four major banks required to share mortgage and personal loan data.
1 February 2021	Non-major ADIs able to share certain types of data under the CDR Banking Rules.
1 July 2021	Non-major ADIs able to share all types of data under the CDR Banking Rules.

Consumer data right (cont'd)

Applying the consumer data right to the energy sector: The Gateway Model and the AEMO

The energy sector will be the next designated sector to implement CDR (expected in latter half of 2020). Whilst the government initially surmised that the energy sector will fall under the same model as the banking sector, the ACCC confirmed this will no longer be the case. After hearing submissions from key stakeholders, it became evident that the present regulatory framework in the energy sector has built high barriers to entry due to incumbents setting excessive price structures. This has diminished energy retailers' abilities to improve their services and resulted in significant retail costs, with inactive consumers paying disproportionate amounts for their electricity usage.

Furthermore, there are multiple parties within the energy sector that may be holding data relating to one consumer, such as retailers, distributors and Commonwealth energy comparator services. Accordingly, identifying the specific data holders for a particular consumer would be a complex task for an ADR. The ACCC therefore decided to adopt a Gateway Model for the energy sector's consumer data rules. This model leverages the Australian Energy Market Operator's (**AEMO**) IT infrastructure that makes it better placed to identify which service providers hold data of a particular consumer. The AEMO thus acts as a pipeline for the flow of data between the data holders and the ADR.

The AEMO will be under certain obligations as a pipeline. For example, it is required to verify an ADR's accreditation via the ACCC's registry before proceeding with a data request.

However, the AEMO exercises a dual capacity, as it may also be a data holder in its capacity as an energy service provider and will therefore be bound by the same regulations as other data holders in this regard.

Civil penalties

The new regime provides penalties for non-compliance. Currently, the CDR Banking Rules provide for fines of up to $250,000 for corporations and $50,000 for individuals who do not comply with their obligations in meeting consumer data requests.

Key takeaways

Companies operating within the financial services, energy and telecommunication sector should consider the following:

- Identify the CDR-data sets and data flows.
- Develop online programming interfaces that meet on-demand requests for consumer data in an efficient and transparent manner.
- Consider technology and third parties that may be of assistance with compliance measures.
- Determine your company's current capability to comply with rules and standards, including implementing privacy safeguards, security measures and consent requirements.
- Consider the compliance requirements that will flow from the CDR and develop a compliance program to prepare for and implement the measures necessary to meet your obligations.
- Consider whether there are new opportunities as a data recipient. If so, develop a business case and strategy around the benefits and costs of CDR participation.

Notable enforcement activity by the ACCC and OAIC

Recent enforcement activity taken by the ACCC and the OAIC demonstrate the regulators' propensity to scrutinise the activities of digital platforms and the importance for organisations to be transparent when processing data. Of particular interest is the dual-regulatory focus and intersection of the Australian Consumer Law and Privacy Act which is impacting the use of data and personal information from a consumer protection law and privacy perspective.

Prosecutions awaiting judgement in Court:

ACCC v Google

In October 2019, the ACCC commenced action against Google LLC and Google Australia Pty Ltd in the Federal Court of Australia for alleged breaches of the Australian Consumer Law (**ACL**).

The ACCC's allegations related to Google's misleading and deceptive representations made to Android device users in relation to the collection and use of customers' location data. In particular:

- On-screen representations made in the Google account set up of which led consumers to incorrectly believe their "Location History" was the only setting that determined Google's collection of their location data when in fact the "Web and App Activity" setting also had to be manually switched off.
- The lack of disclosures provided by Google meant users could not make informed choices as to the sharing of their location data.
- The failure to disclose how the location data may be used by Google for a number of other purposes (which were unrelated to a consumer's use of Google's services) was misleading.

The ACCC is seeking penalties (where the current maximum is $10 million), declarations and corrective notice publication orders, and that Google establish a compliance program. It also follows from other international regulatory action against Google.

OAIC v Facebook

In March 2020, the OAIC commenced proceedings against Facebook in the Federal Court of Australia for alleged repeated and systemic failures to comply with the Privacy Act.

In summary, the OAIC alleges Facebook breached the privacy of around 311,127 Australian Facebook users by not taking reasonable steps to secure the personal information (due to its default settings) and allowing the unauthorised disclosure of their personal information to the **This Is Your Digital Life** app for purposes other than the purpose for which their personal information was collected (in breach of APP 6 and 11). The OAIC alleges Facebook failed to be transparent about the way it handled personal information as most users did not install the app themselves but had their personal information disclosed through their friend's use of the app. In addition, the OAIC alleges Facebook used and sold this personal information to third parties for other purposes including political profiling.

The OAIC is seeking various relief including civil penalties against Facebook (where the current maximum is $1.7 million for serious and/or repeated breaches). This action follows from the Cambridge Analytica events in 2018 and the subsequent international enforcement action taken overseas.

Privacy Act reform

Increased penalties and enforcement powers

In March 2019, the Australian government announced it would amend the *Privacy Act 1988* (Cth) to increase the maximum civil penalties for privacy breaches.

If the proposed amendments are implemented, the OAIC will have the ability to seek penalties for serious or repeated breaches to the higher of $10 million, an amount that is 3 times the value of any benefit obtained through the misuse of information or 10% of a company's annual domestic turnover (up from $2.1 million). These amendments align with the penalties under the Australian Consumer Law and will be met by broader enforcement powers of the OAIC.

Additionally, the OAIC will be able to issue infringement notices of up to $63,000 for bodies corporate and $12,000 for individuals for failure to cooperate with efforts to resolve minor breaches.

The OAIC will develop a binding online privacy code which will be implemented in 2020 to correspond with the increased penalty provisions. This code will apply to social media companies trading in personal information and will require such platforms to meet consent requirements, cease disclosing personal information when instructed by the individual, as well as implement risk management strategies to protect vulnerable groups, including children and the elderly.

All social media platforms and other online companies operating within Australia's digital market should prepare to be heavily scrutinised by regulators in relation to their privacy obligations as enforcement action will be taken if such obligations are not met.

The OAIC's approach to the future of privacy

During the Australian Information Commissioner's address at the 2019 IAPP Summit, it was stated that the OAIC is focused on four key elements for regulating privacy into the future (as set out below).

1	**International Interoperability**	Furthering universal policies, standards and models for privacy protection.
2	**Self-management**	Allowing individuals to exercise control over how their personal information is managed.
3	**Organisational accountability**	Holding organisations accountable for breaches of privacy laws.
4	**Scope of privacy laws**	Broadening the coverage of the Privacy Act to capture businesses that are currently exempt.

Other privacy related reform on the horizon

AI Ethical Framework

The Department of Industry, Innovation and Science (DIIS) released its AI Ethics Principles following its discussion paper dated 5 April 2019. The DIIS published eight voluntary principles that aim to influence organisations using AI to consider the ethical implications that can arise from such use. One of these principles relates to ensuring that privacy rights and data security is preserved throughout an AI machine's lifecycle. Whilst these principles are a positive step forward in addressing the potential implications of AI technology, the Australian Parliament has not been forthcoming in regulating AI ethics. Accordingly, the effectiveness of these principles remains uncertain and in need of further development.

Data Sharing and Release Bill

A draft Data Sharing and Release Act has been released for comment and proposes to streamline the process of sharing data held by government entities. The proposed Act will apply to Commonwealth entities whose data can only be released if it satisfies a 'purpose test' and if certain safeguards are put in place. Data will be shared irrespective of this rule if it is for national security or law enforcement purposes. Whilst the proposed legislation will assist the government in implementing better-informed policies, when enacted, it also enables the government to use data for purposes unknown to the public under the national security exception.

Consumer Loyalty Schemes

Concerns have been raised regarding how corporations' gather and use consumer data from their loyalty schemes. Certain entities have been found collecting data from a consumer's bank card and connecting this data to their loyalty profiles to track spending behaviours. In December 2019, the ACCC made a number of recommendations in its Customer Loyalty Schemes Final Report, including compelling businesses to improve their loyalty scheme privacy disclaimers, prohibiting the linking of consumers' bank cards with loyalty scheme profiles. The ACCC also recommended strengthening the protections within the *Privacy Act 1988* (Cth) by imposing an obligation on entities to immediately erase any personal information of a consumer upon that consumer's request.

Assistance and Access Bill

The *Telecommunications Act 1997* (Cth) has been amended to equip law enforcement and national security agencies with the tools purportedly necessary to protect Australia amidst this digital era. Section 317L of the Act empowers the Director-General of Security or a chief officer of an interception agency to issue a 'technical assistance notice' to a telecommunications provider. The provider will be required to provide access to its encrypted data for the purpose of detecting criminal activity, such as terrorism and human trafficking. The *Criminal Code Act 1995* (the Code) has also been amended. Subsection 474.6(7A) of the Code has been incorporated to ensure providers are not liable for any offences detected from the technical assistance notice.

Voluntary code of practice for IoT

In late 2019, the government released a draft voluntary Code of Practice: Securing the Internet of Things for Consumers (CoP) for comment. The CoP sets out a voluntary suite of measures to be read as 'best practice' guidance for industry to secure consumer Internet of Things (IoT) devices that connect to the internet (i.e. smart TVs, watches and home automation devices/speakers). Key principles include: (i) ensuring manufacturers of these devices do not utilise 'default' or 'weak' passwords to access the device; (ii) the public is able to report vulnerabilities in these systems and the manufacturers have policies in place to ensure these vulnerabilities are dealt with in a timely manner; and (iii) ensuring that software is regularly updated and remains secure.

Key cyber and privacy contacts

For a deeper discussion of how these cyber and privacy-related developments might affect your business or entity, please contact:

Tony O'Malley
Partner, Legal
+61 (2) 8266 3015
tony.omalley@pwc.com

Sylvia Ng
Director & Privacy Lead, Legal
+61 (2) 8266 0338
sylvia.ng@pwc.com

Adrian Chotar
Partner, Legal
+61 (0) 457 808 068
adrian.chotar@pwc.com

Cameron Whittfield
Partner, Legal
+61 (0) 448 101 001
cameron.whittfield@pwc.com

James Patto
Director, Legal
+61 (0) 431 275 693
james.patto@pwc.com

Luke Pigram
Manager, Legal
+61 (7) 3257 5002
luke.pigram@pwc.com

www.pwc.com.au

PwC200079128