PwC International Business Reorganisations Network – Monthly Legal Update

Edition 5, May 2018

Contents

Welcome

Welcome to the fifth edition of the PwC International Business Reorganisations (**IBR**) Network Monthly Legal Update for 2018.

The PwC IBR Network provides legal services to assist multinational organisations with their cross-border reorganisations. We focus on post-deal integration, pre-transaction separation and carve outs, single entity projects, and legal entity rationalisation and simplification as well as general business and corporate and commercial structuring.

Each month our global legal network brings you insights and updates on key legal issues multinational organisations.

We hope that you will find this publication helpful, and we look forward to hearing from you.

In this issue

In our May 2018 issue:

- PwC Legal AG Rechsanwaltsgellschaft (Germany) examines the new European General Data Protection Regulation and its impact on companies and company groups; and
- PricewaterhouseCoopers (Australia) reports on upcoming changes to privacy laws in 2018.

Contact us

For your global contact and more information on PwC's IBR services, please contact:

Richard Edmundson

*Special Legal Consultant**

Managing Partner, ILC Legal, LLP

+1 (202) 312-0877

richard.edmundson@ilclegal.com

** Mr. Edmundson is admitted as a solicitor in England and Wales and is licensed to practice in the District of Columbia as a Special Legal Consultant.*

PwC Legal AG Rechtsanwaltsgesellschaft (Germany) – The EU General Data Protection Regulation

At a glance

The new European General Data Protection Regulation (EU-directive 2016/679) (**GDPR**) intends to centralise data protection matters and at the same time to increase the level of data protection in the European Union (**EU**).

The GDPR was established in 2016, however its provisions will be applicable as of 25 May 2018. In the meantime, EU-based companies, but also companies from outside the EU, had and still have time to implement data protection measures according to the GDPR.

This article provides a short overview on what such companies will have to expect as of 25 May 2018.

Company groups will have to take a closer look at data transfers between group companies and ensure that their internal organisation is compliant with the GDPR. Penalties and fines for the violation of data protection regulations have been increased significantly.

In detail

1. Who is affected by the GDPR?

According to Sec. 1 GDPR the intention of the GDPR is to protect natural persons (not data!) with regard to the processing of personal data (*data subjects*). The GDPR therefore binds any *controller* according to Sec. 4 no. 7 GDPR. Controller means:

> "*the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data*."

Consequently, any company or natural person, no matter the scope under which personal data is being processed, is potentially affected by the GDPR. Data processing is not limited to typical IT-related work, but includes any process, which is performed on personal data.

2. General obligations

The GDPR binds Controllers directly. They are obliged to keep general principles related to processing of personal data (Sec. 5 GDPR), such as *lawfulness, fairness and transparency*, *data minimization*, *accuracy* and *integrity and confidentiality*.

Those principles lead to a huge variety of specific obligations that come with processing data, e.g. documentation (Sec. 5 subsec. 2; 30, 35 GDPR) and information obligations (Sec. 13, 14 GDPR). The controller has to implement:

> "*technical and organisational measures to ensure a level of security appropriate to risk*" (Art. 25, 32 GDPR)."

Further, the controller shall both at the time of the determination of the means for processing and at the time of the processing itself implement appropriate technical and organisational measures, which are designed to implement data-protection principles, especially data minimization (*Privacy by design* and *privacy by default*).

3. Rights of the data subjects

The GDPR strengthens the position of the data subject, moreover, the aforementioned obligations are reflected by respecting rights of the data subject. Sec. 6 GDPR allows the controller only to process personal data under specific circumstances (lawfulness of data processing, see above), the most important being the consent by the data subject (Sec. 6 subsec. 1 sentence 1 lit. a) GDPR) and *legitimate interests pursued by the controller* (Sec. 6 subsec. 1 sentence 1 lit. f) GDPR).

Sec. 12 to 23 GDPR contain the data subjects' rights towards the controller, among others, rights of information, the right of access, right of rectification, right to erasure (the so called *right to be forgotten*) and the right to object. Under certain circumstances, data subjects may have claims for compensation for damages suffered due to the controller's breach of data protection rules.

4. Expanded territorial reach

The GDPR includes controllers and processors outside the EU whose processing activities relate to the offering of goods or services to, or monitoring the behaviour of, EU data subjects (within the EU). This means in practice that a company outside the EU, which is targeting consumers in the EU will be subject to the GDPR.

This leads to non-EU companies being subject to the aforementioned obligations. Many of those non-EU companies will need to appoint representatives in the EU for matters of data protection (Sec. 27 GDPR).

EU-companies that wish to have data processed by foreign companies need to make sure that the GDPR grants such data transfer. This may happen according to Sec. 45 GDPR by an adequacy decision of the European Commission. The European Commission decides if a foreign country or international organisation ensures an adequate level of protection. This happened, for instance, with regard to Argentina, Canada, Israel, New Zealand and Switzerland. The US, however, are not considered adequate data protection wise, which calls for attention in case data is to be transferred there. As for now, companies in the US can submit to the so-called "*EU-US Privacy Shield*", an international agreement by which US companies accept data protection standards and the EU deems such companies adequate according to Sec. 45 GDPR. Since data protection activists in the EU have already placed lawsuits against the EU-US Privacy Shield, it is questionable if it will remain in force and / or unchanged.

5. Effects on company groups

a The One-Stop-Shop mechanism

The so-called *One-Stop-Shop* mechanism is one of the key elements of the GDPR. It means that one national authority is to be the lead data protection authority for a company based in several EU member states. According to Sec. 55 subsec. 1 GDPR the competent authority is determined where the controller or the processor have their headquarter (Sec. 4 No. 16 GDPR).

b Data transfer within a company group

Another issue will be processing and transferring data within a company group: many company groups centralise their administration and require a permanent data transfer to the administrative entity in charge. In the absence of an explicit stipulation in the GDPR, companies within a company group are third parties in relation to each other, thereby creating the need for any data transfer to be lawful, in the meaning as outlined above under No. 3.

Company groups are defined by the GDPR as a

> "*controlling undertaking and its controlled undertakings*".

This may be accomplished by the possession of shares, a financial investment or any other controlling influence. In such constellations, one might find it difficult to determine which entity within a respective company group is to be considered as controller according to the GDPR. In cases involving a parent company with controlling influence (therefore with the power to establish rules and guidelines in matters of data protection) and operative, data processing subsidiaries, the parent company's controlling influence should lead to the conclusion that the parent company is the controller according to the GDPR. This conclusion however leads to problems whenever the parent company is not EU-based: it might then be necessary to appoint a representative within the EU (e.g. one of the EU-based subsidiaries) according to Sec. 27 GDPR; further, the GDPR may prohibit any data transfer to such parent company (see above No. 4).

In case of fully EU-based company groups, European legislation seems to imply the application of the *intra group exemption*, thereby allowing any data transfer within such a company group. However, this assessment is based merely on *Recital 48* of the GDPR, which states that

> "*Controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data*".

The Recitals *consist* of precedent reasons and explanations by the EU Parliament and the Council of the European Union, which are not part of the legal text. However, many companies and law *advisors* interpret this Recital as a legitimate interest pursued by the controller according to Sec. 6 subsec. 1 sentence 1 lit. f) GDPR and therefore as lawful.

6. Penalties / Fines

Violations of obligations under the GDPR will be fined according to Sec. 83 GDPR. Fines have been increased significantly compared to, for instance, the German regulations that will be in force until 25 May 2018. Fines will be placed up to EUR 20,000,000 or 4 % of the worldwide revenue of the affected company (depending which amount is higher. It is unclear, if the worldwide revenue includes the revenue of other group companies, since Sec. 83 GDPR only refers to "*companies*", such being different from "*company groups*", see Sec. 4 subsec. 1 No. 18 and 19 GDPR.

Further, it is to be taken into account that, due to the nature of the applicable German Act on Regulatory Offences, the managing director or any responsible employee of a German Company may be personally responsible as controller and therefore the person being fined (besides the affected company).

Who to contact

For more information, please contact:

Robert Dorr
Local Partner, co-Head of the IBR German legal network, Stuttgart / Munich
+49 711 25034 1505
robert.dorr@pwc.com

Stephan Schaal
Associate, Stuttgart
+49 711 250341724
schaal.stephan@pwc.com

PricewaterhouseCoopers (Australia) – Australian Privacy Outlook 2018

At a glance

This article highlights some key features of impending privacy-related changes that are due to come into effect both in Australia and internationally in 2018, in particular:

a the Australian Notifiable Data Breaches scheme;

b the European Union (**UN**) General Data Protection Regulation;

c the Australian Government Agencies Privacy Code;

d the Consumer Data Right;

e Open Banking; and

f Mandatory Comprehensive Credit Reporting.

In detail

2018 is poised to be a year of change with new, strengthened privacy laws coming into effect both in Australia and internationally; and now that we are well and truly in the swing of the year, the implementation dates for a number of significant changes is fast approaching.

Developments in technology and the ever-increasing volumes and flow of data, have led to an increased focus on cybersecurity, opportunities to commercialise or innovate with data, while maintaining consumer trust and addressing privacy concerns.

Many Australian agencies and organisations are now subject to new obligations under the Australian Notifiable Data Breaches scheme which came into effect on 22 February 2018. In addition, many Australian organisations may also be caught by the extra-jurisdictional reach of the EU's new General Data Protection Regulation (**GDPR**) which comes into effect from 25 May 2018.

There are also sector and industry-specific changes which will impact privacy matters for particular entities, including the mandatory comprehensive credit reporting and open banking regimes, the Australian Government Agencies APP Code, and the Consumer Data Right which is expected to be legislated this year in relation to particular industry sectors.

This paper highlights some key features of these impending privacy-related changes.

1. Notifiable data breaches scheme

The Notifiable Data Breaches scheme (**NDB Scheme**) is set out in Part IIIC of the *Privacy Act 1988* (Cth) (**Privacy Act**) and requires agencies and organisations to report to the Office of the Australian Information Commissioner (**OAIC**) and affected individuals in the event of an '**eligible data breach**'.

PwC's rundown of the NDB Scheme's key features is found **here**.

The NDB Scheme came into effect on 22 February 2018, and in the lead up to its commencement, the OAIC released a number of related guidances (the **Resources**). The Resources provide useful insights into the OAIC's perspectives on interpretation and application of the NDB Scheme which will no-doubt prove useful now that the NDB Scheme is in operation. After two rounds of consultation in 2017, many of these resources are now in final form.

In particular, the Resources provide guidance as to:

a the steps that agencies and organisations should take when **assessing** a suspected data breach;

b the application of certain **exceptions** to the notification requirement;

c the OAIC's expectations of the contents of an eligible data breach **notification**; and

d **regulatory action** that may be taken in respect of data breach incidents.

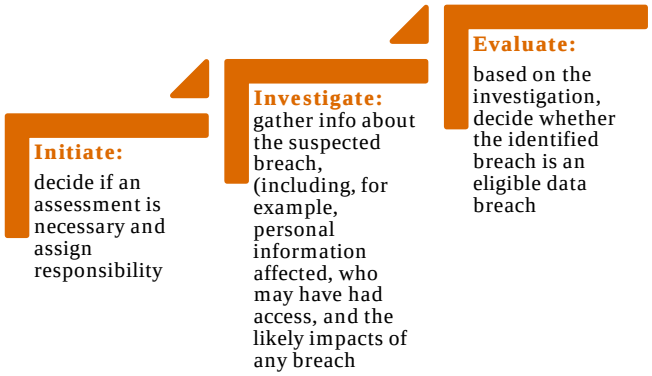
a What happens if there is a suspected data breach?

An entity that is aware that there are reasonable grounds to suspect it may have experienced an eligible data breach must promptly (and within 30 days) assess the situation to determine whether there has been an eligible data breach. The Resources provide the following useful insights to assist with the assessment:

i Whether there are 'reasonable grounds' to suspect a data breach is a factual matter which turns on how a reasonable, properly informed person would act in the circumstances.

ii It is expected that, where possible, entities will complete the assessment of a suspected data breach well within the 30 day limit. If an entity cannot reasonably complete the assessment within the limit, the OAIC recommends the entity documents and demonstrates that: all reasonable steps have been taken to complete the assessment within 30 days, the reasons for the delay and that the assessment was reasonable and expeditious.

iii A risk-based approach should be taken to the assessment, with time and effort spent proportionate to the likelihood of a breach and its apparent severity. The Resources recommend a three-stage assessment process comprising of:



b What information should a notification contain?

The Resources shed some additional light on what must be included in the notification of an eligible data breach to the OAIC and affected individuals:

Entity identity should be the name most familiar to affected individuals (especially where company and trading name are different).

Contact details may include a dedicated phone number or email address where the nature/size of the breach render this appropriate.

Description of the eligible data breach must inform affected individuals sufficiently to assess the possible impacts of the breach, and take protective action in response. This may include the date of breach, date detected, circumstances of the breach, who may have accessed the information, and recommended steps for mitigation.

Kind or kinds of information concerned should be clearly stated, including whether it involved sensitive information.

Recommended steps for mitigation should be a practical recommendation(s) to mitigate the serious harm or likelihood of serious harm arising from the data breach. Appropriate recommendations will depend on the nature of the entity and breach.

Other entities involved in the data breach, including contact details, may be included where appropriate (subject to the nature of the breach and relationship between affected individuals and the entities and between the entities themselves).

The OAIC has made available an **online notification form** to assist entities to prepare a notification (available at **this link**).

c What are the OAIC's expectations in terms of regulatory action?

The Resources clarify certain processes under the NDB Scheme, which may or may not result in the OAIC requiring notification.

Applications to not notify: in certain circumstances, an entity can apply to the OAIC to not have to notify under the NDB Scheme. To be accepted, applications must (among other things) be timely, be in the public interest, sufficiently describe the data breach and the entity's reasons for applying.

Direction requiring notification: the Commissioner can direct an entity to notify affected individuals about an eligible data breach. In notifying individuals, the entity may be asked to specify the risk of harm to individuals, what steps the Commissioner recommends individuals take and how complaints can be made under the Privacy Act.

2. EU General Data Protection Regulation

The GDPR comes into effect on 25 May 2018 and introduces a number of significant, prescriptive privacy changes and obligations. Importantly, it has extra-territorial reach and Australian businesses should carefully consider whether they are caught by this law – with fines of up to €20 million per infringement or 4 per cent of annual global turnover (whichever is greater) set to apply for non-compliance.

Some key compliance requirements of the GDPR include:

a Privacy Notices

i **Increased disclosure requirements** to data subjects before collection of data, particularly if the data subject is a child.

ii Where necessary, the **reissue** of privacy notices to existing customers must be required.

b Consent and legal basis for processing

i More stringent requirements where consent is relied on as **legal basis for processing personal data**.

ii Consent must be freely given, specific, informed and unambiguous.

iii Individuals must be able to easily **withdraw** consent at any time.

iv Several legal bases for processing exist under the GDPR, other than consent.

v The personal data collected should be **limited to what is necessary** for the purposes of processing.

c Sensitive Personal Data

More stringent protections around the collection and processing of sensitive data –it is only allowed in specified circumstances, even if the individual has provided consent.

d Data Breaches

Entities must notify the regulator of any data breach **within 72 hours** of becoming aware of the breach. Any delay must be supported by reasons.

• Affected individuals must also be notified if the breach is likely to cause **a high risk to the individual's rights and freedoms**.

e New Customer Rights

Customers will have the right to **access** their personal data, be **forgotten**, and **restrict the processing** of their personal data.

i For **access** requests, entities must respond to the request within **30 days**.

ii They will also have the right **to data portability**.

f Third Party Contracts

i Changes to the legal relationship between data controllers and processors, including **required contractual provisions** and allocation of responsibility (where there are joint data controllers).

ii Data processors will have direct obligations in respect of their data processing activities; and controllers will have related obligations to ensure that processors conduct the processing compliant with the GDPR.

g Accountability and record keeping

i Controllers and processors must be able to **demonstrate compliance** with the GDPR – usually by way of a 'paper shield'.

ii This may require the **update or creation of policies, procedures, registers** and practical measures implemented to achieve compliance.

h Data protection officer

i In some circumstances entities may be obliged to **appoint a data protection officer** (**DPO**). The GDPR imposes several obligations on the DPO.

ii This is particularly the case where the entity's core activities involve **large scale processing** of certain categories of personal information.

iii Entities which are not subject to the mandatory requirement may **voluntarily** appoint a DPO; but to do so triggers the legal DPO obligations.

i Preparations by Australian entities

There are severe reputational, economic and legal risks arising from non-compliance with the GDPR. With only a few months remaining till the GDPR commences, Australian entities should assess their data flows and operations to determine whether they are subject to the GDPR requirements; and if so, think carefully about actions required to achieve a compliance framework that can withstand adverse scrutiny from a range of stakeholders. For more information on the GDPR and how PwC can assist with your readiness, see **this link**.

3. Australian Government Agencies APP Code

The *Privacy (Australian Government Agencies — Governance) APP Code 2017* (**Government Agencies Code**) takes effect from 1 July 2018. The Government Agencies Code applies to 'agencies' already covered by the Privacy Act and specifies some of the ways in which agencies must comply with Australian Privacy Principle 1.2. Key obligations include:

a Privacy impact assessments

Conduct PIAs for high privacy risk projects. Generally, this is where a project involves new or changed personal information handling, likely to significantly impact individuals' privacy.

A PIA involves a written assessment of how a project might affect individuals' privacy and recommends steps to manage, minimise or eliminate that impact.

b Education and training

Provide training at staff inductions, on the agency's privacy obligations, policies and procedures.

Appropriately educate staff members who access personal information as part of their role.

c Privacy Champion

Designate a senior official as the privacy champion.

Ensure that the privacy champion's functions are carried out, including (without limitation) providing leadership on strategic privacy issues and promoting a culture of privacy.

d Privacy Officer

Appoint at least one privacy officer and provide the OAIC with the officer(s) details.

Privacy Officer must be the key contact for advice on privacy within the agency.

Ensure the privacy officer's functions are carried out, which include (without limitation) handling of privacy enquiries, complaints and access or correction requests and conducting and documenting PIAs.

e Privacy management plan

Identify specific and measurable privacy goals and targets.

Measure and document performance against the Privacy Management Plan (at least annually).

4. Consumer Data Right

a Empowering consumers, increasing innovation and competition

In May 2017, the Productivity Commission's Report on *Data Availability and Use* (**Report**) was released and recommended that a Consumer Data Right be introduced (see our summary of the Report at **this link**).

The recommendation suggested that consumers be granted a right to not only request access for themselves to their personal data, but also to request that it be provided directly to a third party in a **machine readable format**.

The Report further recommended that industry participants of impacted sectors should determine:

i transfer mechanisms and security of data;

ii **scope of consumer data** as relevant to the industry; and

iii requirements necessary to **authenticate** a consumer request **prior** to any **transfer**.

b How will the Consumer Data Right be implemented?

The **banking sector** will be the first to be impacted through the Open Banking regime (see over page), followed by the **telecommunications and energy sectors**. It is envisaged that ultimately, the Consumer Data Right will later be extended to apply to other sectors too.

Participants in the telecommunications and energy sectors should begin considering how they currently hold and secure data, and how it may potentially be transferred to consumers and/or third parties.

There is some semblance between the Consumer Data Right and the 'right to data portability' under the GDPR. So Australian organisations caught by the latter may discover that uplifts to their data systems to comply with the GDPR may satisfy the former. But such comparisons can only meaningfully take place once the Australian Government has legislated this, so as to reveal the more granular aspects of how the mechanics of the Consumer Data Right will operate and be enforced.

c What is the purpose of this right?

The purpose of the Consumer Data Right, as framed in the Report, is two-fold:

i to allow consumers to access and re-use their own data, thereby supporting a social licence for better, economy-wide data use; and

ii underpin a wave of competition policy, by allowing consumers to obtain a copy of their personal data, provided to them and/or a nominated third party.

The Government's announcement, consistent with the Report, theorises that providing individuals with better access to their personal data will empower them to seek out better offers and products, and improve ease of switching providers. At first instance, the Consumer Data Right will allow customers open access to their **banking**, **energy**, **phone** and **internet** transactions.

4. Open Banking

The Open Banking regime is intended to empower customers with a right to access the information they have shared with the banks and have that information securely shared with other parties.

The Australian Government recently released its Report into the *Review of Open Banking*(Open Banking Report, see **here** to access the Open Banking Report), which made several key recommendations on the design and operation of Australia's open banking system.

a Key Changes

i Generally, at a customer's direction, **data holders** such as banks, should be **obliged to share** all information about the customer, free of charge.

ii This represents the Australian Government's **first application** of the **Consumer Data Right**.

b Key Features

i There should be a **multi regulator model**, led by the Australian Competition and Consumer Commission (**ACCC**), with the **OAIC** remaining primarily responsible for **privacy** protection.

ii A **Data Standards Body** should be established to work with regulators to develop standards for data sharing, including **transfer standards**, **data standards** and **security standards**.

iii **Participants**, being holders and recipients of Open Banking data, should be **accredited** by the ACCC.

iv Data transfers between the banks should occur through application programming interfaces.

v All **data recipients** should be subject to the **Privacy Act**. The Australian Privacy Principles (contained in schedule 1 to the Privacy Act) should be uplifted, including more requirements to obtain **express client consent**.

c How will the Consumer Data Right be Implemented?

i Generally, at a customer's direction, **data holders** such as banks, should be **obliged to share** all information about the customer, free of charge.

ii This represents the Australian Government's **first application** of the **Consumer Data Right**.

d Scope of open banking

Open Banking should only apply to digitally held data.

i Open Banking should encompass **customer-provided** data and **transaction** data (in a manner that facilitates its **transfer** and **use**).

ii Open Banking should **not apply** to **aggregated** data, data materially increasing the risk of **identity theft** or **value-added** customer data (being that which is materially enhanced due to insights, analysis or transformation).

e The Takeaway

The exclusion of aggregated and value-added data from Open Banking (if the recommendation is adopted), will prevent banks from having to share proprietary data, and will be a welcome feature in the context of big data analytics. Nonetheless, banks will need to start considering how to arrange their systems to respond to data transfer requests.

5. Mandatory Comprehensive Credit Reporting

Public consultation on the Australian Government's exposure draft of the N*ational Consumer Credit Protection Amendment (Mandatory Comprehensive Credit Reporting) Bill 2018* (Cth) (**Draft Bill**) closed on 23 February 2018. The Draft Bill is available from this link. This regime is part of the quest for responsible lending procedures designed to give credit providers more access to credit information on borrowers in order to properly assess that borrower's financial background, credit history and ability to repay loans.

a Background and aim

Initially, the Privacy Act permitted credit providers to only report 'negative' credit information to credit reporting bodies (**CRBs**), such as an individual's delinquency history. But since March 2014, reforms to the Privacy Act have allowed credit providers to (voluntarily) report 'positive' information too, including the maximum credit available to an individual (**Comprehensive Information**).

The Report found that, despite the reforms, Comprehensive Information reporting has been low.

The Draft Bill proposes to mandate Comprehensive Information reporting, to provide lenders with a deeper, richer set of data to better assess a borrower's true credit position and loan repayment ability.

b Impact on banks

If passed in its current form, the regime will initially only apply to large authorised deposit-taking institutions (those with resident assets exceeding AU$100 billion) (**ADIs**) and their subsidiaries (Eligible Licensees).

Eligible Licensees will be required to report mandatory credit information on 50 per cent of their active and open credit accounts by 28 September 2018. Remaining information, including that which relates to accounts opened on after 1 July 2018, must be supplied by 28 September 2019.

c Incentives for small lenders

CRBs cannot disclose credit information collected under the Draft Bill, to a credit provider unless the credit provider is contributing credit information on its active and open credit accounts.

This measure will incentivise smaller lenders to also report Comprehensive Information.

d Privacy implications

The Draft Bill does not propose to alter existing provisions in the Privacy Act and *Privacy (Credit Reporting) Code 2014 (Version 1.2)* in respect of the **collection** or **sharing** of credit information. But if enacted, the Draft Bill will restrict the circumstances in which a **CRB** can **store** credit information **overseas**.

Further, the Draft Bill will (if enacted) **oblige credit providers** to, prior to supplying information to a CRB, be satisfied that the **CRB's security arrangements** comply with the **Privacy Act**.

e The Takeaway

The Open Banking Regime and mandatory Comprehensive Information reporting could together, materially increase **the compliance burden of lenders**. Affected credit providers should start preparing for the '**first bulk supply**', required by 28 September 2018. With increasing **cloud software usage**, CRBs should ensure that credit information **stored overseas** satisfies the Draft Bill's conditions.

Who to contact

For more information, please contact:

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

Sylvia Ng
Partner, Legal
+61 (2) 8266 0338
sylvia.ng@pwc.com

www.pwc.com