www.pwc.com.au

2018 Australian privacy outlook

LegalTalk Alert

Authors: Sylvia Ng, Steph Baker, Rohan Shukla

12 March 2018

pwc

A privacy focused agenda has arrived

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.

Contents

Notifiable data breaches scheme

What is the 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:

- the steps that agencies and organisations should take when **assessing** a suspected data breach;
- the application of certain **exceptions** to the notification requirement;
- the OAIC's expectations of the contents of an eligible data breach **notification**; and
- **regulatory action** that may be taken in respect of data breach incidents.

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:

- 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.
- 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.
- 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:

Initiate
decide if an assessment is necessary and assign responsibility.

Investigate
gather information about the suspected breach, (including, for example the personal information affected, who may have had access, and the likely impacts of any breach).

Evaluate
on based on the investigation, decide whether the identified breach is an eligible data breach.

Notifiable data breaches scheme (cont'd)

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**).

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.

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:

Privacy notices

- **Increased disclosure requirements** to data subjects before collection of data, particularly if the data subject is a child.
- Where necessary, the **reissue** of privacy notices to existing customers must be required.

Consent & legal basis for processing

- More stringent requirements where consent is relied on as **legal basis for processing personal data**.
- Consent must be freely given, specific, informed and unambiguous.
- Individuals must be able to easily **withdraw** consent at any time.
- Several legal bases for processing exist under the GDPR, other than consent.
- The personal data collected should be **limited to what is necessary** for the purposes of processing.

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.

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**.

New customer rights

- Customers will have the right to **access** their personal data, be **forgotten,** and **restrict the processing** of their personal data.
- For **access** requests, entities must respond to the request within **30 days**.
- They will also have the right **to data portability**.

EU General Data Protection Regulation (cont'd)

Third party contracts

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

Accountability and record keeping

- Controllers and processors must be able to **demonstrate compliance** with the GDPR – usually by way of a 'paper shield'.
- This may require the **update or creation of policies, procedures, registers** and practical measures implemented to achieve compliance.

Data protection officer

- In some circumstances entities may be obliged to **appoint a data protection officer** (**DPO**). The GDPR imposes several obligations on the DPO.
- This is particularly the case where the entity's core activities involve **large scale processing** of certain categories of personal information.
- Entities which are not subject to the mandatory requirement may **voluntarily** appoint a DPO; but to do so triggers the legal DPO obligations.

Preparations by Australian entities

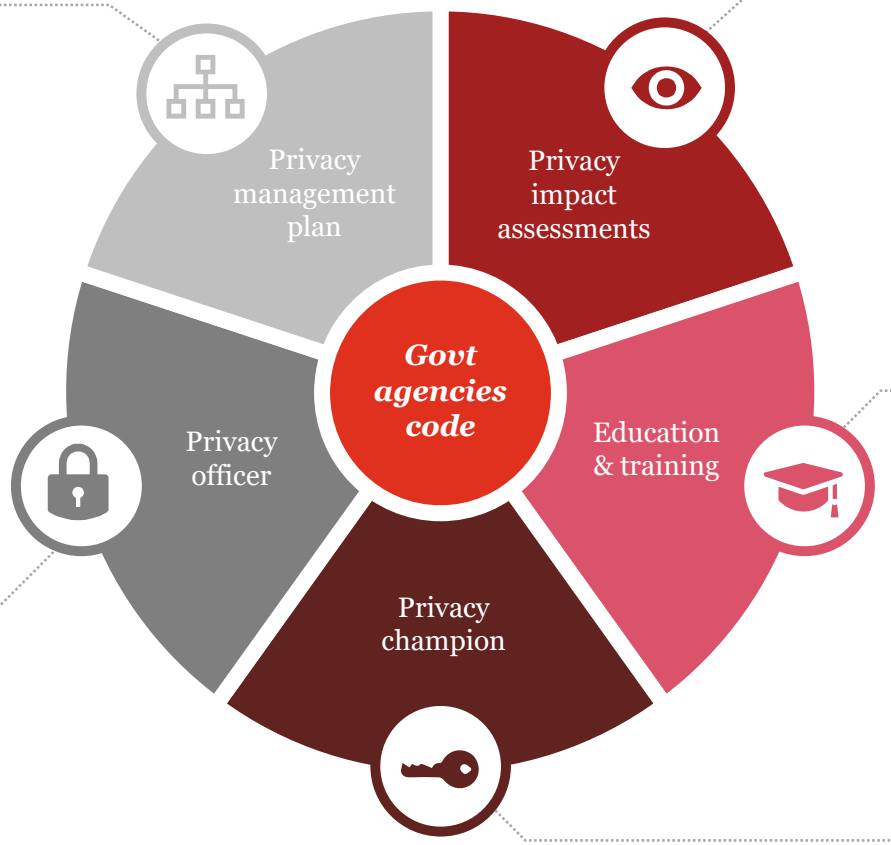
There are severe reputational, economic and legal risks arising from non-compliance with the GDPR. With only a few months remaining till the GDPR commences, Australian entities should assess their data flows and operations to determine whether they are subject to the GDPR requirements; and if so, think 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**.

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:

- Identify specific and measurable **privacy goals** and **targets**.
- **Measure and document performance** against the Privacy Management Plan (at least annually).

- 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**.



- 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.

- 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.

- 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.**

The Government Agencies Code increases the accountability of agencies under the Privacy Act. Particularly, agencies will need to ensure that their organisational structure facilitates the fulfilment of functions of the privacy officer(s) and privacy champion.

Consumer Data Right

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:

- **transfer mechanisms** and **security** of data;
- **scope of consumer data** as relevant to the industry; and
- requirements necessary to **authenticate** a consumer request **prior** to any **transfer**.

In November 2017, the Australian Government announced its intention to legislate for a Consumer Data Right for certain industry sectors in 2018

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.

What is the purposes of this right?

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

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

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.

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.

Key changes

- Generally, at a customer's direction, **data holders** such as banks, should be **obliged to share** all information about the customer, free of charge.
- This represents the Australian Government's **first application** of the **Consumer Data Right**.

Key features

- 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.
- 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**.
- **Participants**, being holders and recipients of Open Banking data, should be **accredited** by the ACCC.
- Data transfers between the banks should occur through application programming interfaces.
- 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.**

How will the Consumer Data Right be implemented?

- Generally, at a customer's direction, **data holders** such as banks, should be **obliged to share** all information about the customer, free of charge.
- This represents the Australian Government's **first application** of the **Consumer Data Right**.

Scope of open banking

- Open Banking should only apply to digitally held data.
- Open Banking should encompass **customer-provided** data and **transaction** data (in a manner that facilitates its **transfer** and **use**).
- 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).

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.

Mandatory Comprehensive Credit Reporting

Public consultation on the Australian Government's exposure draft of the *National 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.

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.

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**.

Incentives for smaller 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.

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**.

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.

Let's talk...

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

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

Adrian Chotar
Partner, Legal
+61 (2) 8266 1320
adrian.chotar@pwc.com

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

Steph Baker
Financial Advisory, Legal
+61 (2) 8266 5054
Steph.baker@pwc.com

Rohan Shukla
Financial Advisory, Legal
+61 (2) 8266 5591
rohan.shukla@pwc.com

www.pwc.com.au

127058737