

The new Australian Notifiable Data Breach Scheme

Peter Leonard¹
Principal, Data Synergies

1 Introduction

A Notifiable Data Breaches (**NDB**) scheme will operate in Australia from 22 February 2018.

The scheme only applies to eligible data breaches that occur on, or after, that date in Australia.

The NDB scheme requires organisations covered by the Australian (federal) Privacy Act 1988 (**Privacy Act**) to notify any individuals likely to be at risk of serious harm by a data breach. This notice must take a prescribed form and must include recommendations about the steps that individuals should take in response to the data breach. The Office of the Australian Information Commissioner (**OAIC**), being the office of the Australian Privacy Commissioner (**Commissioner**), must also be notified.

Examples of a data breach include when:

- a device containing customers' personal information is lost or stolen,
- a database containing personal information is hacked, or
- personal information is mistakenly provided to the wrong person.

An 'eligible data breach' arises when the following three criteria are satisfied:

- there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds, and
- this is likely to result in serious harm to one or more individuals to whom the information relates, and
- the entity has not been able to prevent the likely risk of serious harm with remedial action.

Under the NDB scheme, if personal information is lost in circumstances where subsequent unauthorised access to or disclosure of the information is unlikely, there is no eligible data breach.² For example, if the personal information is remotely deleted before an unauthorised person could access the information, or if the information is encrypted to a high standard making unauthorised access or disclosure unlikely, then there is no eligible data breach.

'Serious harm' is not defined in the Privacy Act. In the context of a data breach, serious harm to an individual may include serious physical, psychological, emotional, financial, or reputational harm. Examples may include:

- identity theft,
- significant financial loss by the individual,

¹ Peter Leonard is a data, content and technology business consultant and lawyer and principal of Data Synergies. Peter chairs the IoTAA's Data Access, Use and Privacy work stream. The IoT Alliance (www.iot.org.au) is Australia's peak IoT body, bringing together industry government and regulators to address issues affecting IoT adoption and implementation. Peter also chairs the Law Society of New South Wales' Privacy and Data Committee and the Australian Computer Society's Artificial Intelligence and Ethics Technical Committee. He serves on a number of relevant advisory boards, including of the NSW Data Analytics Centre. Peter was a founding partner of Gilbert + Tobin, now a large Australian law firm. Following his retirement as a partner in 2017 he continues to assist Gilbert + Tobin as a consultant. This paper was last revised on 12 February 2018.

² s 26WE(2)(b)(ii)

- threats to an individual's physical safety,
- loss of business or employment opportunities,
- humiliation, damage to reputation or relationships,
- workplace or social bullying or marginalisation.

The likelihood of a particular harm occurring, as well as the anticipated consequences for individuals whose personal information is involved in the data breach if the harm materialises, are relevant considerations.

The following summary of the NDB scheme does not address various details such as available exceptions and exemptions. It is a general guide only. The summary extensively draws upon guidance provided by the Commissioner.³

2 Which entities must notify NDBs?

In general terms, agencies and organisations (entities) that are already covered by the Privacy Act must comply with the Notifiable Data Breaches (NDB) scheme. More precisely, the scheme applies to entities that have an obligation under APP 11 of the Privacy Act to protect the personal information they hold.⁴ Collectively known as 'APP entities', these include most Australian Government agencies, some private sector and not-for-profit organisations (Australian Privacy Principle (APP) entities, credit reporting bodies, credit providers, and tax file number (TFN) recipients), and all private health service providers.

The definition of 'APP entity' generally does not include small business operators, registered political parties, state or territory authorities, or a prescribed instrumentality of a state (s 6C). A small business operator (**SBO**) is an individual (including a sole trader), body corporate, partnership, unincorporated association, or trust that has not had an annual turnover of more than \$3 million in any financial year since 2001.⁵ Generally, SBOs do not have obligations under the APPs unless an exception applies.⁶ However, if an SBO falls into one of the following categories, that SBO is not exempt and must comply with the APPs, and therefore with the NDB scheme, in relation to all of the SBO's activities:

- entities that provide health services, including small businesses that provide a health service and hold people's health information. This generally general practitioners (GPs), pharmacists, therapists, allied health professionals, gyms and weight loss clinics, and childcare centres, among others,⁷
- entities related (through majority ownership or effective control) to an APP entity,
- entities that trade in personal information,
- credit reporting bodies,
- employee associations registered under the Fair Work (Registered Organisations) Act 2009, and
- entities that 'opt-in' to APP coverage under s 6EA of the Privacy Act.

In addition, if an SBO carries on any of the following activities it must comply with the APPs, and therefore must comply with the NDB scheme, but only in relation to personal information held by the SBO for the purpose of, or in connection with, those activities:

- providing services to the Commonwealth under a contract,

³ As at <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme>.

⁴ s 26WE(1)(a)

⁵ s 6D

⁶ s 6D(4)

⁷ <https://www.oaic.gov.au/media-and-speeches/news/gps-gyms-and-childcare-centres-may-have-obligations-under-the-notifiable-data-breaches-scheme-will-your-organisation>

- operating a residential tenancy data base,
- reporting under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006,
- conducting a protected action ballot, and
- retention of information to comply with requirements of the mandatory data retention scheme, as per Part 5-1A of the Telecommunications (Interception and Access) Act 1979.

Overseas data breaches

If an APP entity discloses personal information to an overseas recipient that is not regulated as an APP entity, in line with the requirements of APP 8, then the APP entity is deemed to 'hold' the information for the purposes of the NDB scheme.⁸ APP 8 says that an APP entity that discloses personal information to an overseas recipient is generally required to ensure that the recipient will comply with the APPs when handling that information. Importantly, this means that if the personal information held by the overseas recipient is subject to unauthorised access or disclosure, the APP entity is still responsible for assessing whether it is an eligible data breach under the Privacy Act, and if it is, for notifying the Commissioner and individuals at risk of serious harm.

Multiple entities

Two or more entities may hold the same personal information in a number of circumstances, including when an entity outsources the handling of personal information, is involved in a joint venture, or where it has a shared services arrangement with another entity.

If an eligible data breach involves personal information held by more than one entity, only one of the entities needs to notify the Commissioner and individuals (s 26WM).

The NDB scheme does not specify which entity must notify, in order to allow entities flexibility in making arrangements appropriate for their business and their customers.

Entities should consider making arrangements regarding compliance with NDB scheme requirements, including notification to individuals at risk of serious harm, such as in service agreements or other relevant contractual arrangements, as a matter of course when entering into such agreements.

Other cross border issues

The Privacy Act applies to businesses that is established or incorporated in Australia (subject to the small business exemption) and Australian (federal) government agencies even when they are conducting activities outside Australia.

Accordingly, the Privacy Act has extraterritorial reach. Individuals whose personal information is protected by the Privacy Act need not be Australian citizens or Australian residents. The operation of the Privacy Act is generally tied to the status of the entity engaging in a particular act or practice, and/or the location in which an entity engages in that act or practice.

For example, where an APP entity is regulated in relation to its acts or practices outside Australia (generally being where it is a businesses established or incorporated in Australia, or an Australian (federal) government agency), those acts or practices must conform with the requirements of the Privacy Act, regardless of requirements of local law in the jurisdiction where the act or practice occurs. Generally, compliance with local law in a foreign country where the act or practice occurs, including pursuant to any law of that foreign country, does not excuse non-compliance by an APP entity with the Privacy Act. However, an act or practice outside Australia will not breach the APPs if the act or practice is both engaged in outside Australia and required by an applicable law of a foreign country.

⁸ s 26WC(1)

Each entity within a corporate group is generally considered separately, although related bodies corporate are treated together for limited purposes.

The Privacy Act also regulates as an ‘APP entity’ a businesses outside Australia if that entity carries on a business in Australia and the relevant personal information is collected or held by the organisation or operator in Australia or an external Territory, either before or at the time of the act or practice.⁹ Accordingly, such entities are relevantly regulated only in relation to personal information collected or held by the organisation or operator in Australia or an external Territory, but not other personal information handled by such entities.

3 Making an assessment

The relevant thresholds

If an entity is aware of reasonable grounds to believe that there has been an eligible data breach, it must promptly prepare a statement about the eligible data breach for the Commissioner and notify individuals at risk of serious harm.

If an entity only has reason to suspect that there may have been a serious breach, it must to move quickly to resolve that suspicion by assessing whether an eligible data breach has occurred. If, during the course of an assessment, it becomes clear that there has been an eligible breach, then the entity needs to promptly comply with the notification requirements.

The requirement for an assessment is triggered if and when an entity is aware that there are reasonable grounds to suspect that there may have been a serious breach.¹⁰

The Commissioner’s guidance states:

“Whether an entity is ‘aware’ of a suspected breach is a factual matter in each case, having regard to how a reasonable person who is properly informed would be expected to act in the circumstances. For instance, if a person responsible for compliance or personnel with appropriate seniority are aware of information that suggests a suspected breach may have occurred, an assessment should be done. An entity should not unreasonably delay an assessment of a suspected eligible breach, for instance by waiting until its CEO or Board is aware of information that would otherwise trigger reasonable suspicion of a breach within the entity.

The OAIC expects entities to have practices, procedures, and systems in place to comply with their information security obligations under APP 11, enabling suspected breaches to be promptly identified, reported to relevant personnel, and assessed if necessary.”¹¹

Multiple entities are affected

If a data breach affects one or more other entities, and one entity has assessed the suspected breach, the other entities are not required to also assess the breach.¹² If no assessment is conducted, depending on the circumstances, each entity that holds the information may be found to be in breach of the assessment requirements. The NDB scheme does not prescribe which entity should conduct the assessment in these circumstances. Entities should establish clear arrangements where information is held jointly, so that assessments are carried out quickly and effectively.

⁹ s 5B(3)

¹⁰ s 26WH(1); see also OAIC, Assessing a suspected data breach, <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/assessing-a-suspected-data-breach>; OAIC, Identifying eligible data breaches, December 2017, <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/identifying-eligible-data-breaches>

¹¹ OAIC, OAIC, Assessing a suspected data breach, <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/assessing-a-suspected-data-breach>

¹² s 26WJ

An entity must take all reasonable steps to complete the assessment within 30 calendar days after the day the entity became aware of the grounds (or information) that caused it to suspect an eligible data breach.¹³ The OAIC expects that “wherever possible entities treat 30 days as a maximum time limit for completing an assessment, and endeavour to complete the assessment in a much shorter timeframe, as the risk of serious harm to individuals often increases with time”.¹⁴

Where an entity cannot reasonably complete an assessment within 30 days, OAIC recommends that it should document this, so that the entity it is able to demonstrate:

- that all reasonable steps have been taken to complete the assessment within 30 days,
- what were the reasons for delay, and
- the assessment was reasonable and expeditious.¹⁵

4 How and when is a NDB notified?

Notice to whom?

Entities are also required to prepare a statement (a ‘Notifiable Data Breach Form’) and provide a copy to the Australian Information Commissioner. The statement must include the name and contact details of the entity, a description of the eligible data breach, the kind or kinds of information involved, and what steps the entity recommends that individuals at risk of serious harm take in response to the eligible data breach.¹⁶ A form is available.¹⁷

Entities must also notify individuals as soon as practicable after completing the statement prepared for notifying the Commissioner.¹⁸

Considerations of cost, time, and effort may be relevant in deciding an entity’s decision about when to notify individuals. However, the Commissioner generally expects entities to expeditiously notify individuals at risk of serious harm about an eligible data breach, unless cost, time, and effort are excessively prohibitive in all the circumstances. If entities have notified individuals at risk of serious harm of the data breach before they notify the Commissioner, they do not need to notify those individuals again, so long as the individuals were notified of the contents of the statement given to the Commissioner. The scheme does not require that notification be given to the Commissioner before individuals at risk of serious harm, so if entities wish to begin notifying those individuals before, or at the same time as notifying the Commissioner, they may do so.

The Notifiable Data Breaches (NDB) scheme allows three options for notifying individuals at risk of serious harm, depending on what is ‘practicable’ for the entity.¹⁹

Option 1 — Notify all individuals²⁰

If it is practicable, an entity can notify all of the individuals to whom the relevant information relates.

This option may be appropriate if an entity cannot reasonably assess which particular individuals are at risk of serious harm from an eligible data breach that involves personal information about many people, but where the entity has formed the view that serious harm is likely for one or more of the individuals.

¹³ s 26WH(2)

¹⁴ OAIC, Assessing a suspected data breach, <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/assessing-a-suspected-data-breach>

¹⁵ ibid

¹⁶ s 26WK(3)

¹⁷ <https://forms.uat.business.gov.au/smartforms/landing.htm?formCode=OAIC-NDB>

¹⁸ s 26WL(3)

¹⁹ See further OAIC, Notifying individuals about an eligible data breach, December 2017, <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/notifying-individuals-about-an-eligible-data-breach>

²⁰ s 26WL(2)(a)

The benefits of this approach include ensuring that all individuals who may be at risk of serious harm are notified, and allowing them to consider whether they need to take any action in response to the data breach.

Option 2 — Notify only those individuals at risk of serious harm²¹

If it is practicable, an entity can notify only those individuals who are at risk of serious harm from the eligible data breach(es).

If an entity identifies that only a particular individual, or a specific subset of individuals, involved in an eligible data breach is at risk of serious harm, and can specifically identify those individuals, only those individuals need to be notified. The benefits of this targeted approach include avoiding possible notification fatigue among members of the public, and reducing administrative costs, where it is not required by the NDB scheme.

The Commissioner provides the following example:

“An attacker installs malicious software on a retailer’s website. The software allows the attacker to intercept payment card details when customers make purchases on the website. The attacker is also able to access basic account details for all customers who have an account on the website. Following a comprehensive risk assessment, the retailer considers that the individuals who made purchases during the period that the malicious software was active are at likely risk of serious harm, due to the likelihood of payment card fraud. Based on this assessment, the retailer also considers that those customers who only had basic account details accessed are not at likely risk of serious harm. The retailer is only required to notify those individuals that it considers to be at likely risk of serious harm.”²²

Option 3 – Publish notification²³

If neither option 1 or 2 above are practicable, the entity must:

- publish a copy of the statement on its website (if the entity has one), and
- take reasonable steps to publicise the contents of the statement.

Entities must also take proactive steps to publicise the substance of the data breach (and at least the contents of the statement), to increase the likelihood that the eligible data breach will come to the attention of individuals at risk of serious harm.

An entity can notify an individual using their usual method of communicating with that particular individual.²⁴

Form and content of the notification

The entity can tailor the form of its notification to individuals, which may or may not be in the form given to the Commissioner²⁵, so long as long as the notification to individuals includes the content of the statement required by s 26WK, being:

- the identity and contact details of the entity²⁶

²¹ s 26WL(2)(b)

²² OAIC, Notifying individuals about an eligible data breach, December 2017, <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/notifying-individuals-about-an-eligible-data-breach>

²³ s 26WL(2)(c)

²⁴ s 26WL(4)

²⁵ <https://forms.uat.business.gov.au/smartforms/landing.htm?formCode=OAIC-NDB>

²⁶ s 26WK(3)(a)

- a description of the eligible data breach that the entity has reasonable grounds to believe has happened²⁷
- the kind, or kinds, of information concerned,²⁸ and
- recommendations about the steps that individuals should take in response to the data breach.²⁹

The Commissioner has stated that the OAIC expects that the statement will include sufficient information about the data breach to allow affected individuals the opportunity to properly assess the possible consequences of the data breach for them, and to take protective action in response.³⁰ Information describing the eligible data breach may include:

- the date of the unauthorised access or disclosure,
- the date the entity detected the data breach,
- the circumstances of the data breach (such as any known causes for the unauthorised access or disclosure),
- who has obtained or is likely to have obtained access to the information, and
- relevant information about the steps the entity has taken to contain the breach.

The Commissioner provides the following example:

“For example, to help reduce the risk of identity theft or fraud, recommendations in response to a data breach that involved individuals’ Medicare numbers might include steps an individual can take to request a new Medicare card. Or in the case of a data breach that involved credit card information, putting individuals at risk of identity theft, recommendations might include that an individual contact their financial institution to change their credit card number, and also contact a credit reporting body to establish a ban period on their credit report.”³¹

Multiple entities

When a data breach affects more than one entity, the entity that prepares the statement may include the identity and contact details of the other entities involved.³² Whether an entity includes the identity and contact details of other involved entities in its statement will depend on the circumstances of the eligible data breach, and the relationship between the entities and the individuals involved. The Privacy Act does not require this information to be included on the statement, and it is open to entities to assess whether it is useful to provide this information to individuals.

The Commissioner suggests that, in general, the entity with the most direct relationship with the individuals at risk of serious harm should notify. This will allow individuals to better understand the notification, and how the eligible data breach might affect them. The Commissioner provides the following example:

“A medical practice stores paper-based patient records with a contracted storage provider. The storage provider’s premises are broken into, and the patient records stolen. While the storage provider cannot immediately determine if the stolen items included the medical practice’s records, it suspects that they might have been included. Both the medical practice and the storage provider hold the records for the purpose of the Privacy Act, so both have an obligation to conduct an

²⁷ s 26WK(3)(b)

²⁸ s 26WK(3)(c)

²⁹ 26WK(3)(d)

³⁰ OAIC, What to include in an eligible data breach statement, December 2017, <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/what-to-include-in-an-eligible-data-breach-statement>

³¹ Ibid

³² s 26WK(4)

assessment and, if required, notify. Since the storage provider is more familiar with its facilities, the entities decide that the storage provider is best placed to conduct an assessment and determine if the records were stolen. Once the provider determines that the records were stolen, the medical practice assists the assessment by using its knowledge about the affected individuals to conclude that serious harm is likely. Although the storage provider's insurance company has agreed to cover the cost of notification, the storage provider and medical practice agree that it is most appropriate that notification come from the medical practice, as the relevant individuals do not have any pre-existing relationship with the storage provider. As such, the medical practice notifies the individuals about the incident and is reimbursed by the storage provider and its insurer for the costs of notification."³³

The Commissioner recognises that in some instances the identity and contact details of a third party may not be relevant to an individual whose personal information is involved in an eligible data breach: for example, where the individual does not have a relationship with the other entity. In these circumstances, rather than include the identity and contact details of the third party or parties, the entity that prepares the statement may wish to describe the commercial relationship with the third party in its description of the data breach.

When must the notification be given?

Entities must prepare and give a copy of the statement to the Commissioner as soon as practicable after becoming aware of the eligible data breach.³⁴

What is a 'practicable' timeframe will vary depending on the entity's circumstances, and may include considerations of the time, effort, or cost required to prepare the statement. The Commissioner has stated that the OAIC expects that once an entity becomes aware of an eligible data breach, the entity will provide a statement to the Commissioner promptly, unless there are circumstances that reasonably hinder the entity's ability to do so.

5 Continuing operation of APP 11

APP 11 - *security of personal information* requires APP entities to take reasonable steps to protect personal information they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure. APP 11 states:

11.1 If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:

- a. from misuse, interference and loss; and
- b. from unauthorised access, modification or disclosure.

11.2 If:

- a. an APP entity holds personal information about an individual; and
- b. the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under this Schedule; and
- c. the information is not contained in a Commonwealth record; and
- d. the entity is not required by or under an Australian law, or a court/tribunal order, to retain the information;

³³ OAIC, Data breaches involving more than one organisation, December 2017, <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/data-breaches-involving-more-than-one-organisation>

³⁴ s 26WK(2)

the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.

Other provisions of the Privacy Act create equivalent obligations in relation to credit reporting information, credit eligibility information and tax file number information.

APP 11 has been the subject of useful guidance from the Australian Information Commissioner, most notably:

- OAIC, *APP Guidelines*, Chapter 11: APP 11 — Security of personal information³⁵; and
- OAIC, *Guide to securing personal information*, January 2015.³⁶

The NDB scheme supplements the operation of APP 11.

Before February 2018 the OAIC already received voluntary data breach notifications. The OAIC received 114 voluntary data breach notifications in the July 2016 - June 2017 financial year, a 7% increase from 107 notifications the preceding financial year.³⁷

The OAIC is already responsible for mandatory data breach notifications under the *My Health Records Act* 2012 (formerly known as the Personally Controlled Electronic Health Records (**PCEHR**) scheme.

6 International standards for data breach notification?

In many circumstances an APP entity conducting cross-border business may be required to notify affected individuals and regulatory authorities in Australia and one or more other jurisdictions, including European Union countries. Australian businesses need to be aware of the separate thresholds and time limits that will apply in different jurisdictions.

There is no international standard for data breach notification or the jurisdictional nexus or other locating factors that give rise to an obligation to notify in a particular jurisdiction. Often a data breach may need to be notified in multiple jurisdictions, in markedly different forms, even if the intrusion or other event that give rise to the obligation to notify occurred in only one jurisdiction. Sometimes the obligation will arise independently from the laws of the jurisdiction within which the intrusion or other event that give rise to the obligation to notify occurred.

Care should be taken in developing international data breach response plans to ensure that national variants are addressed.

United States of America

In the U.S.A., the US Congress has repeatedly attempted, but failed, to agree on federal data breach notification legislation. As a result, there is no single federal statute that imposes a breach notification obligation on most companies. 'Reasonable' security standards are still being debated. Nearly every U.S. state has a different breach notification law, with widely varying notification thresholds. 48 states and the District of Columbia have each passed their own laws that require notifications in certain circumstances. Alabama and South Dakota are the only states without breach notification laws.³⁸

Many U.S. state data breach laws state a trigger for notification to the data protection authority of likelihood or possibility of fraud or identity theft or other significant adverse consequence for affected individuals within the relevant state.

³⁵ <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-11-app-11-security-of-personal-information>

³⁶ <https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information>

³⁷ Office of the Australian Information Commissioner *Annual Report 2016–2017*, page 10

³⁸ <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>

Canada

In Canada, the *Digital Privacy Act* of June 2015³⁹ amended Canada's federal private sector privacy law, the *Personal Information Protection and Electronic Documents Act (PIPEDA)*. While other provisions of the Digital Privacy Act are now in force, those dealing with breach reporting, notification and recordkeeping will come into force after regulations outlining specific requirements are developed and in place.

On September 2, 2017, the Government of Canada published proposed 'Breach of Security Safeguards Regulations'.⁴⁰ The proposed regulations relate to the PIPEDA provisions not yet in force.

The PIPEDA provisions when in force will require an organization to notify affected individuals, and report to the Office of the Privacy Commissioner of Canada (**OPC**), as soon as feasible, regarding any data breach which poses a "real risk of significant harm" to any individual whose personal information was involved in the breach. The breach provisions in PIPEDA specify that such notification and reporting must be done in accordance with regulations passed pursuant to PIPEDA.

Failure to notify the OPC of a security breach, as required by the PIPEDA provisions yet to come into force, is an offence, punishable by a fine of up to \$100,000. PIPEDA also contains a private right of action for affected individuals, which could result in damages being awarded by the Federal Court of Canada for failure to notify affected individuals. This private right of action also opens the door to potential class actions for an organization's failure to comply with the breach notification provisions in PIPEDA.

The proposed Breach Regulations specify that reports to the OPC must be in writing and must contain certain stipulated information, such as a description of the circumstances of the breach, the date or time period of the breach, an estimate of the number of affected individuals, a description of the steps taken to reduce the risk of harm, and a description of the organization's notification or intended notification steps.

Notification to affected individuals must include similar information as provided to the OPC, and must also include:

- a toll-free number or email address that affected individuals can use to obtain further information about the breach; and
- information about the organization's internal complaint process and about the affected individual's right to file a complaint with the OPC.

Acceptable methods of direct and indirect notification to individuals are also set out in the proposed Breach Regulations. Indirect notification may be given in circumstances such as where the giving of direct notification would cause further harm to the affected individual, where the organization does not have the current contact information for affected individuals, or where the cost of giving direct notification is prohibitive for the organization.

European Union

The new General Data Protection Regulation (**GDPR**) will introduce mandatory data breach notification across the European Union. The Article 29 Working Party⁴¹ has recently completed a comment period on Guidelines on Personal data breach notification under Regulation 2016/679.⁴² As at 12 February 2018 the Guidelines were adopted but not yet finalised.

Under Article 3 of the GDPR, a business (wherever resident and whether or not located in the EU or processing in the EU) controls or processes personal data of individuals in the EU if the processing is related to offering goods or services into the EU or monitoring the behaviour of individuals in the EU.

³⁹ Available through https://www.priv.gc.ca/resource/fs-fi/02_05_d_63_s4_e.asp

⁴⁰ <http://www.gazette.gc.ca/rp-pr/p1/2017/2017-09-02/html/reg1-eng.php>

⁴¹ http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

⁴² http://ec.europa.eu/newsroom/document.cfm?doc_id=47741

For the purposes of the GDPR, a data ‘controller’ determines the purposes and means of collection of personal data, and the ‘processor’ processes the information on their behalf.

“Processing” is not a concept of Australian privacy law. The term is broadly defined and essentially means any act or practice that is done to, or in connection with, personal information. In considering application of the GDPR, a business needs to review whether it:

- has an ‘establishment’ in the EU? (Article 3.1),
- offers good or services to individuals who are in the EU (whether or not for charge) (Article 3.2(a)), or
- monitors any behaviour of individuals in the EU (Article 3.2(b)).

Article 4 provides that the main establishment of a data controller is the “place of its central administration”: that is, where “decisions on the purposes and means of the processing” occur. For processors, the main establishment will be either the place of central administration in the EU or, if the processor does not have one, then where the main processing activity in the EU takes place.

The GDPR recitals explain that a range of factors will be relevant to deciding whether a company is “offering goods or services” to individuals in the EU. These factors include:

- the use of language and currency or a top-level domain name of an EU Member State,
- delivery of physical goods to a Member State,
- making references to individuals in a Member State to promote the goods and services, and
- targeting advertising at individuals in a Member State.

Mere accessibility of an Australian company's website or app to individuals in the EU will not, by itself, reach the threshold.

Factors relevant to whether a processing activity is ‘monitoring’ the behaviour of individuals in the EU include whether a business is:

- associating individuals in the EU with online identifiers provided by their devices, applications, tools and protocols, such as IP addresses and cookie identifiers,
- tracking their behaviour on the Internet, and
- using data processing techniques that profile individuals, particularly in order to make decisions concerning them for analysing or predicting their personal preferences, behaviours and attitudes.

A “personal data breach” is notifiable⁴³ by a data controller to the relevant data protection authority “without undue delay and, where feasible, not later than 72 hours after having become aware of it”. The WP29 expressed a view that that a controller should be regarded as having become “aware” when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised. If notification is not made within 72 hours, the controller must provide a “reasoned justification” for the delay.

Whenever a breach affects the personal data of individuals in more than one Member State and notification is required, the controller will need to notify the lead supervisory authority, being the supervisory authority of the main establishment or of the single establishment of the controller. Therefore, when drafting its breach

⁴³ Notification to the authority must “at least”: (1) describe the nature of the personal data breach, including the number and categories of data subjects and data records affected; (2) provide the data protection officer's contact information; (3) “describe the likely consequences of the personal data breach”; and (4) describe how the controller proposes to address the breach, including any mitigation efforts. If not all information is available at once, it may be provided in phases.

response plan, a controller must make an assessment as to which supervisory authority is the lead supervisory authority that it will need to notify.

The GDPR provides that when a data processor experiences a personal data breach, it must notify the data controller.⁴⁴ A data processor otherwise does not have relevant notification or reporting obligations under the GDPR.

If a data controller determines that the personal data breach “is likely to result in a high risk to the rights and freedoms of individuals”, the data controller must also communicate information regarding the personal data breach to affected data subjects. Under Article 32, this must be done “without undue delay”. The GDPR provides exceptions to this additional requirement to notify affected data subjects in the following circumstances:

- the controller has “implemented appropriate technical and organisational protection measures” that “render the data unintelligible to any person who is not authorized to access it, such as encryption”;
- the controller takes actions subsequent to the personal data breach to “ensure that the high risk for the rights and freedoms of data subjects” is unlikely to materialize; or
- when notification to each data subject would “involve disproportionate effort”, in which case alternative communication measures may be used.⁴⁵

A “personal data breach” is “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed”. Note that unlike many data breach notification schemes, the requirements extend to destruction of data, or alteration of data, and not just disclosure of personal data information: as the Article 29 Working Party states it, to any of:

- a “confidentiality breach” - where there is an unauthorised or accidental disclosure of, or access to, personal data,
- an “availability breach” - where there is an accidental or unauthorised loss of access to, or destruction of, personal data, and
- an “integrity breach” - where there is an unauthorised or accidental alteration of personal data loss.⁴⁶

However, Article 31(1) contains an exception to the general requirement for notification to the data protection authority of “personal data breach”: notice is not required if “the personal data breach is unlikely to result in a risk for the rights and freedoms of individuals”.

The relevant data protection authority may require notification, or conversely, determine (in effect, confirm) that it is unnecessary under the circumstances.

The GDPR includes large fines: up to 1,000,000 Euros or, in the case of an enterprise, up to two percent of its annual worldwide turnover.

Singapore

Section 24 of the Personal Data Protection Act obliges an organisation to protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

Under the Personal Data Protection Act as at February 2018, there is no explicit requirement for organisations to notify individuals in the event of a data breach. However, the Personal Data Protection

⁴⁴ Article 33(2)

⁴⁵ See Opinion 03/2014 on breach notification; also Guidelines on Personal data breach notification under Regulation 2016/679, pages 15 and 16

⁴⁶ Opinion 03/2014 on breach notification; also Guidelines on Personal data breach notification under Regulation 2016/679, pages 6 and 7.

Commission (PDPC) 'Guide to Managing Data Breaches' provides that it is good practice to notify individuals affected by a data breach.

The PDPC also considers the following as mitigating factors in the event of a breach:

- whether the organisation informed individuals of the steps they could take to mitigate risk caused by a data breach; and
- whether the organisation voluntarily disclosed the personal data breach to the PDPC as soon as it learned of the breach and cooperated with the PDPC's investigation.

However, Singapore is planning introduction of a mandatory data breach notification scheme.⁴⁷ In brief:

- The proposal by the PDPC is to mandate breach notification to both individuals and the PDPC under certain circumstances.
- In cases where there is a risk of impact or harm to the affected individuals, organizations should notify both the individuals and the PDPC.
- However, even when there is no risk of impact or harm to the affected individuals but where the scale of the breach is significant because it involves 500 or more individuals, then the PDPC only must be notified.
- The proposed timeframe for breach notification to the PDPC is 72 hours. For notification to individuals, no specific time frame is provided but they should be notified as soon as practicable.
- In the case of a data intermediary, there will be a requirement to immediately notify the organization on whose behalf it is processing the personal data the event of a breach.
- These notification obligations will operate concurrently with other laws which apply to organizations such as financial institutions and critical infrastructure providers who have obligations to notify regulators under those laws. For example, on July 1 2014 the Monetary Authority of Singapore instructed financial institutions to report all security breaches within one hour of their discovery.

Peter G Leonard

Principal, Data Synergies
Consultant, Gilbert + Tobin

M +61 411 089 003

E pleonard@datasynergies.com.au

LI <https://www.linkedin.com/in/peleonard/>

12 February 2018

⁴⁷ Public Consultation for Approaches to Managing Personal Data in the Digital Economy 27 July 2017 <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Legislation-and-Guidelines/publicconsultationapproachestomanagingpersonaldatainthedigitaleconomy270717f95e65c8844062038829ff000.pdf>