International Standards for Data Breach Notification?

In this second part of a two-part article, Peter Leonard looks at data breach notification regimes in comparative jurisdictions and considers the challenges which arise where a data breach occurs across multiple jurisdictions.

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 counties. 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.[1]

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

Canada

In Canada, the *Digital Privacy Act* of June 2015[2] 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'.[3] The proposed regulations relate to the PIPEDA provisions not yet in force.

The PIPEDA provisions when in force will require an organisation 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 organisation'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 organisation'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

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

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

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

- information about the organisation'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 organisation does not have the current contact information for affected individuals, or where the cost of giving direct notification is prohibitive for the organisation.

European Union

The new General Data Protection Regulation (**GDPR**) will introduce mandatory data breach notification across the European Union. The Article 29 Working Party[4] has recently completed a comment period on Guidelines on Personal data breach notification under Regulation 2016/679.[5] 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.

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 notifiable[6] 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 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 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.[7] A data processor otherwise does not have relevant notification or reporting obligations under the GDPR.

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

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

6 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.

7 Article 33(2)

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 materialise; or

- when notification to each data subject would "involve disproportionate effort", in which case alternative communication measures may be used.[8]

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 scheme, 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.[9]

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 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.[10] 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, organisations 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 organisation 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 organisations 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 Leonard is the Principal at Data Synergies and a Consultant at Gilbert + Tobin.

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

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

10 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