



Australian Government
Attorney-General's Department

December 2015

Discussion paper

Mandatory data breach notification

Discussion paper: mandatory data breach notification

Introduction

The Government agreed to introduce a mandatory data breach notification scheme, and to consult on draft legislation, in response to the February 2015 inquiry of the Parliamentary Joint Committee on Intelligence and Security (PJICIS) into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014.

The Australian Law Reform Commission's (ALRC) 2008 report *For Your Information: Australian Privacy Law and Practice* described mandatory data breach notification as, 'in essence, a legal requirement on agencies and organisations to notify individuals when a breach of security leads to the disclosure of personal information'¹.

The rationale of data breach notification is to allow individuals whose personal information has been compromised in a data breach to take remedial steps to avoid potential adverse consequences, such as financial loss or identity theft. Examples might include cancelling a credit card, or changing an online password.

The ALRC recommended introducing a mandatory data breach notification scheme that would apply to data breaches which create a 'real risk of serious harm' to affected individuals. The previous Government introduced a mandatory data breach notification bill in 2013 based on the ALRC recommendation, but the bill did not pass during the life of that Parliament.

At present, Australian Privacy Principle (APP) 11 in the *Privacy Act 1988* requires government agencies and businesses subject to the Act to take reasonable steps to secure personal information they hold, but does not mandate notification following a data breach. Mandatory data breach notification is required only in the event of unauthorised access to eHealth information under the *My Health Records Act 2012*.

The national privacy regulator, the Office of the Australian Information Commissioner (OAIC), administers a voluntary data breach notification scheme based on the ALRC recommendation (including the 'real risk of serious harm' notification threshold). The OAIC publishes guidelines on how entities subject to the Privacy Act should manage data breaches, and how to assess the risk of harm to individuals following a data breach.

The OAIC received 110 voluntary data breach notifications in 2014-15, up from 67 notifications in 2013-14 and 61 in 2012-13.² The OAIC's enquiries into voluntary data breach notifications focus on the nature of a breach (such as the kind of personal information involved, and how the breach occurred), and the steps taken to contain the breach, mitigate harm to affected individuals, and improve security practices in future. However, the OAIC does not have specific powers to deal with data breaches.

¹ ALRC 108, 2008, *For your information: Australian Privacy Law and Practice*, [51.1].

² OAIC, 2015, *Annual Report 2014-15*, p 58.

The exposure draft of the Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 published alongside this discussion paper is based on the ALRC recommendation. A draft Explanatory Memorandum is also included to explain how the draft Bill is intended to operate if passed into law. Finally, a Regulatory Impact Statement sets out the general policy problem the Bill addresses, explains why the Bill is the preferred solution to that problem at this stage, explores the expected regulatory impact on business, and seeks to consult on general and specific regulatory matters.

This paper contains a brief summary of the draft Bill and compares the proposed scheme with schemes in other jurisdictions. The Government seeks feedback on the draft Bill, Explanatory Memorandum and Regulatory Impact Statement to help finalise a Bill to present before Parliament, with the goal of introducing a data breach notification scheme that protects individual privacy without placing an unreasonable regulatory burden on business.

Have your say

Submissions on the attached exposure draft of the Privacy Amendment (Notification of Serious Data Breaches) Bill 2015, Explanatory Memorandum and Early Assessment Regulatory Impact Statement are sought by **4 March 2016**.

The Government will consider all submissions received in the process of preparing a final draft Bill to present before Parliament.

The preferred method of receiving submissions is via email to privacy.consultation@ag.gov.au, using the submission template on the Attorney-General's Department website at <http://www.ag.gov.au/Consultations/Pages/serious-data-breach-notification.aspx>.

Written submissions can also be sent to:

Commercial and Administrative Law Branch
Attorney-General's Department
3-5 National Circuit
BARTON ACT 2600

Publication of submissions

In meeting the Australian Government's commitment to enhancing the accessibility of published material, the Attorney-General's Department will only publish submissions to this website that have been submitted electronically.

If submitters choose to provide a separate document instead of using the submission template, the following formats are preferred:

- Microsoft Word
- Rich Text Format (RTF)
- txt format.

Please limit individual file size to less than 5MB. The department may create PDF documents from the above formats.

The department will still consider hardcopy submissions received by mail, but these submissions will not be published on the website.

Confidentiality

Submissions received may be made public on the Attorney-General's Department website unless otherwise specified. Submitters should indicate whether any part of the content should not be disclosed to the public. Where confidentiality is requested, submitters are encouraged to provide a version that can be made available.

Australian and international data breach notification arrangements

Existing Privacy Act security requirements

The Australian Privacy Principles (APPs) in the Privacy Act apply to most Australian Government agencies and to private sector organisations with over \$3 million in annual turnover (subject to some exceptions, such as small businesses that are private health service providers or that sell or purchase personal information). Entities falling under the APPs are known as ‘APP entities’.

APP 11 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. Other provisions of the Privacy Act create equivalent obligations in relation to credit reporting information, credit eligibility information and tax file number information.

Structure of draft Bill

The draft Bill would amend the Privacy Act to insert a new Part IIIC, which would define when a ‘serious data breach’ occurs and explain when and in what form notification of serious data breaches is required.

For a detailed explanation of how the new Part IIIC is intended to operate, refer to the draft Explanatory Memorandum published alongside this discussion paper. The remainder of the paper provides a summary and flowcharts explaining how the draft Bill would work, and a table comparing the draft Bill with data breach notification schemes internationally.

Summary — how the draft Bill’s proposed scheme would operate

Commencement date

- The draft Bill’s mandatory data breach notification scheme would commence 12 months after the Bill receives Royal Assent.

Scope and definitions

- Notification to the Australian Information Commissioner (the Commissioner) and affected individuals would only be required following a ‘serious data breach’.
- A serious data breach would occur if:
 - personal information
 - credit reporting information
 - credit eligibility information, or
 - tax file number information

that an entity holds about one or more individuals is subject to unauthorised access or unauthorised disclosure that puts any of the individuals to whom the information relates at **‘real risk of serious harm’**.

- A serious data breach would also occur following the loss of any of the above information, if that loss is likely to lead to unauthorised access or unauthorised disclosure that would put any of the individuals to whom the information relates at real risk of serious harm.

- The draft Bill identifies several relevant matters that entities could take into account when deciding if a real risk of serious harm existed (for example, if the information would be intelligible to other parties). Entities could also take into account any other matters that are relevant in the circumstances.
- It is expected that the Commissioner would issue guidance material to help entities assess whether a 'serious data breach' has occurred, and how to comply with the proposed scheme's notification requirements.
- The proposed scheme would only apply to entities and kinds of information that are subject to existing security requirements in the Privacy Act. For example, the scheme would not apply to:
 - any business not covered by the Privacy Act
 - State and Territory government agencies, or local councils
 - information not regulated by the Privacy Act.

When notification would be required

- Entities would be required to notify the Commissioner and affected individuals if there are reasonable grounds to believe that a serious data breach has occurred. An entity who failed to become aware of a serious data breach that they reasonably should have detected would not be compliant with their notification obligations.
- Where an entity suspected but was not certain that a serious data breach had occurred, the entity would have 30 days to assess whether notification is required. If the assessment found that there are not reasonable grounds to believe a serious data breach has occurred, notification would not be required.
- Where the Commissioner believed that an entity has experienced a serious data breach, but the entity had not notified the breach, the Commissioner could direct the entity to undertake notification. This discretion would be expected to operate in cases where an entity fails to comply with its notification obligations.
- An entity notifying affected individuals would be required to take such steps (if any) as are reasonable in the circumstances to notify each individual. Entities could notify affected individuals using whatever channels they normally use to contact those individuals (for example, email, post, phone).
- Sometimes it might be reasonable for an entity to take no steps to notify each affected individual – for example, if it was not possible to identify each individual, if the entity did not hold contact details for each individual, or if the cost of notifying each individual would be excessive in all of the circumstances.
- Where it would not be practicable to notify each affected individual, the entity would be required to publish a notice about the data breach on the entity's website (if they have one), and take reasonable steps to publicise the notice (for example, through a social media post or an advertisement in online or print media).

Exceptions

- Exceptions would apply for law enforcement purposes, if a secrecy provision in another law applied, or if a breach fell under the existing eHealth mandatory data breach notification scheme under section 75 of the My Health Records Act.
- Entities would also be able to apply to the Commissioner for an exemption if they believed that a serious data breach had occurred but that notification would be contrary to the public interest.

Enforcement and review rights

- Failure to comply with notification obligations would fall under the Privacy Act's existing enforcement and civil penalties framework. For example, the Commissioner could investigate non-compliance, issue a binding determination if necessary, or in the event of serious or repeated non-compliance, apply to the Federal Court or Federal Circuit Court to impose a civil penalty.
- Entities would be able to seek review in the Administrative Appeals Tribunal if the Commissioner directed them to notify a serious data breach, or refused to grant an exemption.

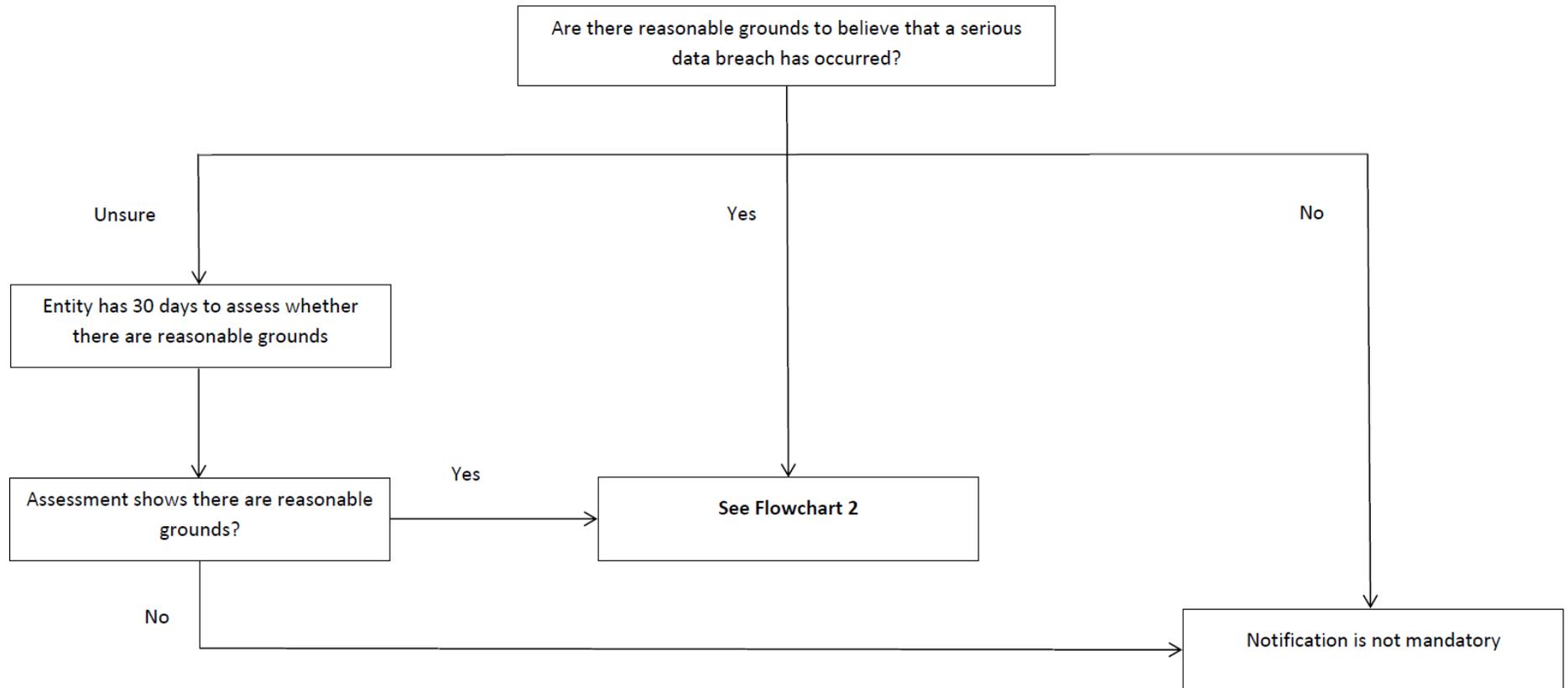
Interaction with the Data Retention Act

- Section 187LA of the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Data Retention Act), which commenced on 13 October 2015, provides that:
 - Telecommunications service providers with data retention obligations under the Data Retention Act are taken to be organisations subject to the Privacy Act to the extent that the activities of the service provider relate to retained data.
 - Retained telecommunications data is taken to be 'personal information' about an individual for the purposes of the Privacy Act if it relates either to the individual or a communication to which they were a party.
- This means that the draft mandatory data breach notification Bill would apply to all telecommunications service providers subject to the Data Retention Act, in relation to data collected and retained under that Act.

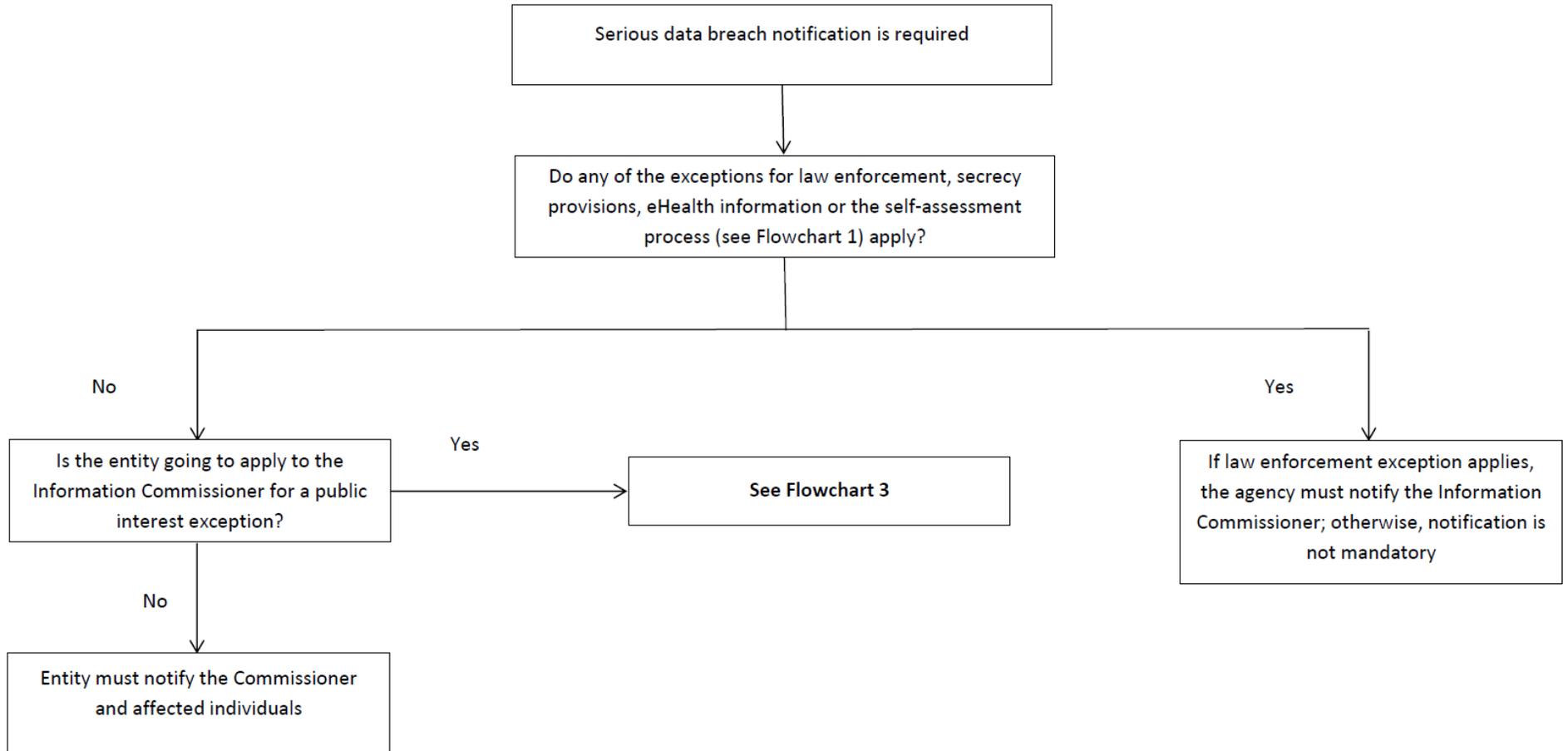
Flowcharts — summary description of how the draft Bill would work

[Alternative text descriptions](#) follow the flowcharts.

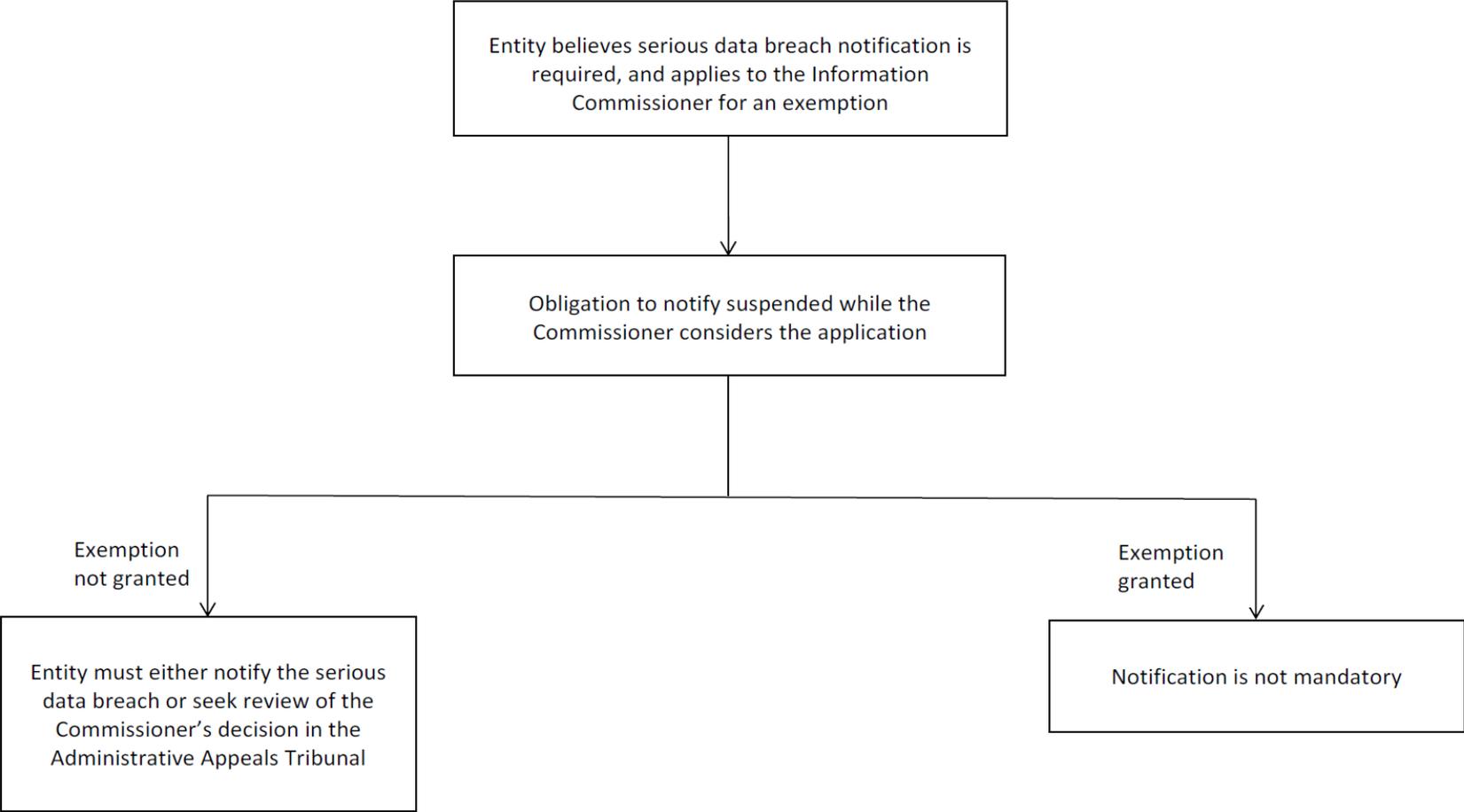
Flowchart 1: determining whether a serious data breach has occurred



Flowchart 2: how to notify a serious data breach



Flowchart 3: applying for an exemption from notification following a serious data breach



Flowchart alternative text descriptions

Flowchart 1: determining whether a serious data breach has occurred

- Are there reasonable grounds to believe that a serious data breach has occurred?
 - Unsure: entity has 30 days to assess whether there are reasonable grounds. If assessment shows there are reasonable grounds, see Flowchart 2; if not, notification is not mandatory.
 - Yes: see Flowchart 2.
 - No: notification is not mandatory.

Flowchart 2: notifying a serious data breach

- Serious data breach notification is required.
- Do any of the exceptions for law enforcement, secrecy provisions, eHealth information or the self-assessment process (see Flowchart 1) apply?
 - No: is the entity going to apply to the Information Commissioner for a public interest exemption? If yes, see Flowchart 3; if not, the entity must notify the serious data breach to the Commissioner and affected individuals.
 - Yes: if the law enforcement exception applies, the agency must notify the Information Commissioner; otherwise, notification is not mandatory.

Flowchart 3: applying for an exemption from notification following a serious data breach

- Entity believes serious data breach notification is required, and applies to the Information Commissioner for an exemption.
- Obligation to notify suspended while the Commissioner considers the application.
 - Exemption not granted: entity must either notify the serious data breach or seek review of the Commissioner's decision in the Administrative Appeals Tribunal.
 - Exemption granted: notification is not mandatory.

Comparison between draft Bill and international data breach notification schemes

Mandatory data breach notification laws apply in the European Union (including the United Kingdom) and 47 American states (many of which have implemented schemes based to some extent on Californian legislation that commenced in 2003). Canada has also passed a mandatory data breach notification law which is yet to commence.

New Zealand and the United States have announced an intention to introduce mandatory data breach notification laws. For New Zealand, mandatory data breach notification would replace an existing voluntary scheme, while the draft United States legislation would replace the variety of existing state data breach notification laws that apply to private sector organisations.

The OECD Privacy Guidelines also state that notice to an authority of a data breach is necessary where there is a significant security breach affecting personal data. The OECD recommends that member countries (including Australia) comply with the Guidelines, but they are not mandatory.

The following table compares the draft Australian bill with existing or proposed mandatory data breach notification schemes in other jurisdictions. In summary, the table shows that the scheme in the draft Australian Bill:

- has a relatively higher notification threshold than schemes in many other jurisdictions, in that notification would only be required in serious cases (which would help avoid the risk of individuals experiencing ‘notification fatigue’, and will also help avoid unnecessary administrative costs for business)
- would be simpler than many actual or proposed schemes in other jurisdictions, in that it does not contain a two-tier scheme where some kinds of breaches must only be notified to a regulator, and other kinds to both the regulator and affected individuals, and
- would be equally as flexible as schemes in other jurisdictions which recognise that data breaches involving adequately encrypted information will pose a lesser risk of harm to affected individuals.

Table 1: Summary international comparison – mandatory data breach notification schemes

Country	Relevant law/instrument/other details	Notification threshold and recipient/s	Kind of information	Consequences for non-compliance	Standard (compared to draft Bill)
Australia — proposed scheme	Exposure Draft — Privacy Amendment (Notification of Serious Data Breaches) Bill 2015	Notify the Information Commissioner and affected individuals of all data breaches creating a real risk of serious harm	Personal information, credit reporting information, credit eligibility information and tax file number information, as defined in the Privacy Act	Risk of enforcement action, including potential civil penalties for serious or repeated infringements	N/A
Canada — scheme passed into law in June 2015 but is yet to commence	Digital Privacy Act	Notify the Privacy Commissioner and affected individuals of all data breaches creating a real risk of significant harm	Personal information, defined as information about an identifiable individual	Risk of fines for knowing or wilful failure to report a breach to the Commissioner, to notify an individual or to maintain records in specified circumstances	Similar
European Union	Commission Regulation (EU) No 611/2013	Notify a national authority of all ‘personal data breaches’ Notify both a national authority and individuals where the data breach is likely to adversely affect the individuals’ personal data or privacy	Personal data, defined so that the notification requirement applies only to providers of publicly available electronic communication services	Judicial remedies and penalties in relevant Member State laws (for example, in the United Kingdom, monetary penalties may apply under the <i>Privacy and Electronic Communications (EC Directive) Regulations 2003</i> or the <i>Data Protection Act 1988</i>)	Lower notification threshold, but applies to a narrower range of information Two-tier notification system

Country	Relevant law/instrument/other details	Notification threshold and recipient/s	Kind of information	Consequences for non-compliance	Standard (compared to draft Bill)
New Zealand — proposed scheme	Outlined in Government press release 'Privacy law changes to strengthen protection', 28 May 2014 ³	Notify all 'material' data breaches to the Privacy Commissioner Notify both the Privacy Commissioner and affected individuals where the breach carries a real risk of harm	Personal information, defined to mean information about an identifiable individual	Expected that Commissioner will have full range of existing powers available	Lower notification threshold Two-tier notification system
OECD Guidelines — international guidance material (not binding)	<i>OECD Privacy Framework</i> (2013)	Notify a national authority of 'significant security breaches' Notify both a national authority and individuals where a significant security breach is likely to adversely affect those individuals	Personal data, defined as information relating to an identified or identifiable individual	N/A	Lower notification threshold Two-tier notification system

³ <http://www.beehive.govt.nz/release/privacy-law-changes-strengthen-protection>.

Country	Relevant law/instrument/other details	Notification threshold and recipient/s	Kind of information	Consequences for non-compliance	Standard (compared to draft Bill)
United States — California	California Civil Code § 1798.29(a) and 1798.82(a) (many other US states have implemented variations on this model)	Notify an individual if their unencrypted personal information is acquired without authority Notify the Attorney General if a data breach affects more than 500 individuals	Personal information, defined as an individual's name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: <ul style="list-style-type: none"> • social security number • drivers' license number • account number, credit or debit card number in combination with an access code • medical information • health insurance Information Any combination of a user name or email address and access credentials also falls under the definition	Criminal penalties and ability under law to sue breaching organisations	Lower notification threshold, but applies to a narrower range of information Encryption provisions similar to how the draft Bill deals with assessing the risk of harm Two-tier notification system

Country	Relevant law/instrument/other details	Notification threshold and recipient/s	Kind of information	Consequences for non-compliance	Standard (compared to draft Bill)
United States — proposed federal scheme	<p>Draft legislation — Personal Data Notification & Protection Act⁴</p> <p>(would replace existing state-based laws applying to the private sector)</p>	<p>Businesses that handle ‘sensitive personally identifiable information’ of more than 10,000 individuals per year must notify an individual of a security breach of that information within 30 days, unless there is no reasonable risk of harm or fraud, or the information is adequately encrypted</p>	<p>Sensitive personally identifiable information, defined (in summary) as an individual’s name in combination with any two of the following:</p> <ul style="list-style-type: none"> • home address, telephone number, mother’s maiden name or birthday • various government identifiers • biometric data • account identifier • user name or electronic mail address, in combination with an access code. <p>Any combination of an individual’s name, account identifier/user name and access credentials also falls under the definition</p>	<p>Attorney-General of the State or the local law enforcement agency on behalf of the residents of the agency’s jurisdiction may bring a civil action</p> <p>The Federal Trade Commission may also commence an investigation</p>	<p>Lower notification threshold with a set time limit, but applies to a narrower range of information</p> <p>Applies only to businesses, not government agencies</p> <p>Encryption provisions similar to how the draft Bill deals with assessing the risk of harm</p> <p>Exclusion of small businesses would potentially be similar to the Australian Privacy Act.</p>

⁴ <https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-data-breach-notification.pdf>