Chapter 9: Data breach incidents

Contents

Notifiable Data Breaches (NDB) scheme

9.1 The OAIC administers a Notifiable Data Breaches (NDB) scheme under Part IIIC of the Privacy Act.

9.2 Under Parts IIIC and VIIIA, entities that have information security obligations under the Privacy Act[1] must generally notify individuals or consumers in relation to CDR data, whose information was involved and the Australian Information Commissioner (the Commissioner), about eligible data breaches (ss 26WK and 26WL and s 94S).

9.3 The Commissioner has the following functions under the scheme:

- offering advice and guidance to regulated entities, and providing information to the community about the operation of the scheme.
- promoting compliance with the scheme
- receiving notifications from entities
- directing an entity to notify under s 26WR
- declaring that notification need not be made, or that notification be delayed under s 26WQ

9.4 Section 56ES(1) and (2) of the Competition and Consumer Act provides that Part IIIC of the Privacy Act applies to accredited data recipients or designated gateways in relation to their

[1] For more information see Entities covered by the NDB scheme

handling of CDR data, within the CDR scheme. This means data breaches within the CDR scheme, that relate to the handling of CDR consumers (including individuals and small businesses), must be reported to the OAIC and are subject to the same requirements of Part IIIC of the Privacy Act.

9.5 There are specific requirements relating to the COVIDSafe app and COVID app data under Part VIIIA of the Privacy Act. Those specific requirements are outlined separately below.

Promoting compliance with the scheme

9.6 Section 13(4A) of the Privacy Act provides that if an entity contravenes any of the following requirements of the NDB scheme, the contravention is taken to be an act that is an interference with the privacy of an individual, subject to possible enforcement action:

- carry out an assessment of a suspected eligible data breach (s 26WH(2))
- prepare a statement about the eligible data breach, and give a copy to the Commissioner as soon as practicable (s 26WK(2))
- notify the contents of the statement to individuals whose personal information was involved in the eligible data breach (or, in certain circumstances, publish the statement) as soon as practicable (s 26WL(3))
- comply with a direction from the Commissioner to notify the eligible data breach (s 26WR(10)).

9.7 The OAIC has developed guidance about the NDB scheme to assist entities.

9.8 The Commissioner may, on the Commissioner's own initiative, investigate an act or practice that may be an interference with privacy where the Commissioner thinks it is desirable to do so (s 40(2)). The Commissioner must also investigate complaints made by individuals where an act or practice may be an interference with the privacy of the individual (s 40(1)).

9.9 Where the Commissioner has identified an interference with privacy, there are a number of enforcement powers available to the Commissioner, ranging from less serious to more serious regulatory action depending on the relevant factors. These include powers to:

- accept an enforceable undertaking (s 80V of the Privacy Act and s 114 of the Regulatory Powers Act) and bring proceedings to enforce an enforceable undertaking (s 115 of the Regulatory Powers Act)
- make a determination (s 52) and bring proceedings to enforce a determination (ss 55A and 62)
- seek an injunction to prevent ongoing activity or a recurrence (s 80W)
- apply to a court for a civil penalty order for a breach of a civil penalty provision (s 80U), which includes serious or repeated interferences with privacy.

9.10 In deciding whether an investigation or enforcement action is appropriate in the circumstances, the Commissioner will act in accordance with the OAIC's *Privacy regulatory action policy*, and the *CDR regulatory action policy* where applicable.

Receipt of notifications

9.11 The Commissioner will acknowledge receipt of all data breach notifications.

9.12 The Commissioner may or may not take any action in response to a data breach notification. The Commissioner will decide which notifications to respond to depending on available resources, and the Commissioner's evaluation of the extent to which taking action in response to the notification will further the objects of the Privacy Act and the objects of Part IVD of the Competition and Consumer Act for the CDR scheme where appropriate.

9.13 Some notifications may point to a possible interference with privacy. Under s 42, the Commissioner may make preliminary inquiries to determine whether to investigate an act or practice that may be an interference with privacy, or in relation to the CDR scheme, that may be a breach of a privacy safeguard or a privacy or confidentiality related Rule, where there has been a complaint or on the Commissioner's own initiative. In deciding whether to make preliminary inquiries or offer advice and guidance in response to a notification, the Commissioner may consider:

- the type and sensitivity of the personal information involved
- the numbers of individuals or CDR consumers potentially at risk of serious harm
- whether the data breach has been contained or is in the process of being contained where feasible
- steps the notifying entity has taken, or is taking, to mitigate the impact on individuals or CDR consumers at risk of serious harm
- measures that the entity has taken, or is taking, to minimise the likelihood of a similar breach occurring again.

9.14 The Commissioner may also inquire about the incident to determine whether the OAIC can provide assistance to the entity, such as best practice advice on data breach responses and the prevention of similar incidents in the future.

Declaration of Commissioner — exception to notification (s 26WQ)

9.15 The Commissioner may declare that an entity does not need to comply with the notification requirements in the NDB scheme in relation to an eligible data breach. Under s 26WQ the Commissioner may give written notice declaring that a statement to the Commissioner (under s 26WK) and notification to individuals or CDR consumers (under s 26WL) is not required,[2] or that notification to individuals or CDR consumers is delayed for a specified period.[3]

9.16 The Commissioner must not make a declaration unless satisfied that it is reasonable in the circumstances to do so, having regard to:

- the public interest (s 26WQ(3)(a))
- any relevant advice given to the Commissioner by an enforcement body or the Australian Signals Directorate (ASD) (s 26WQ(3)(b)),[4] and
- such other matters (if any) as the Commissioner considers relevant (s 26WQ(3)(c)).

[2] Under s 26WQ(1)(c).

[3] Under s 26WQ(1)(d).

[4] The Commissioner may be given such advice or the Commissioner may or may not request such advice.

9.17 An entity that is considering applying to the Commissioner for a s 26WQ declaration should do so as soon as practicable after the entity is aware that there are reasonable grounds to believe an eligible data breach has occurred.

9.18 In deciding whether to make a declaration, and on what terms, the Commissioner will have regard to the objects of the Privacy Act and other relevant matters. The Commissioner will consider whether the risks associated with notifying of a particular data breach outweigh the benefits of notification to individuals or CDR consumers at risk of serious harm.

9.19 Given the clear objective of the scheme to promote notification of eligible data breaches, and the inclusion of exceptions in the scheme that remove the need to notify in a wide range of circumstances, the Commissioner expects that declarations under s 26WQ will only be made in exceptional cases and only after a compelling case has been put forward by the entity seeking the declaration.

Applying for a s 26WQ declaration

9.20 An entity considering making an application under s 26WQ should contact the OAIC in the first instance to discuss its intention.

9.21 If the entity decides to make an application, it should provide the following information and documents to the OAIC:

- a detailed description of the data breach
- a statement outlining the entity's reasons for seeking a s 26WQ notice
- a draft notice setting out the terms that it believes should be included in the notice issued by the Commissioner
- relevant supporting documents and evidence (including, if applicable, relevant advice from an enforcement body or the ASD)
- contact details of an employee or representative of the entity.

9.22 The onus is on the entity to demonstrate to the Commissioner that it is appropriate for the Commissioner to make a declaration. As such, the entity applying for a declaration will be expected to make a well-reasoned and compelling case detailing how the data breach is an eligible data breach, why any relevant exceptions do not apply, and why notification should not occur or should be delayed. The entity should provide detailed evidence or information in support of its application.

9.23 The Commissioner may seek further information from the entity or third parties. However, given the time critical nature of data breach notifications, the entity may not have a further opportunity to provide evidence or submissions to the OAIC before the Commissioner makes a decision on the application. As such, the entity should include all relevant information in its written application.

9.24 In considering whether to make a declaration, the Commissioner will have regard to relevant factors which may include:

- the objects in s 2A of the Privacy Act and the objects of the CDR scheme in Part IVD of the Competition and Consumer Act (set out in s 56AA) if applicable
- the purposes of the NDB scheme, which include enabling individuals (and in the case of the CDR scheme, CDR consumers) to take steps to protect themselves from serious harm arising from a data breach

- the circumstances of the eligible data breach
- the extent to which notification will cause harm to particular groups or to the community at large
- the extent to which benefits of notification will be lost or diminished if notification does not occur or is delayed
- whether advice from an enforcement body or the ASD indicates that notification would be contrary to the public interest in the effective conduct of enforcement related activities or national security matters
- whether the entity responsible for the eligible data breach has been the subject of prior compliance or regulatory enforcement action by the OAIC, and the outcome of that action
- whether the eligible data breach is an isolated instance, or whether it indicates a potential systemic issue (either within the entity concerned or within an industry) or a potential issue which may pose ongoing compliance or enforcement issues
- such other matters as the Commissioner considers relevant.

9.25 After considering the application, the Commissioner will make one of the following decisions:

- a declaration that notification does not need to occur
- a declaration that notification can be delayed (either for the period proposed by the applicant, or another period selected by the Commissioner)
- a refusal of the application.

9.26 Where the Commissioner refuses a declaration, the Commissioner will give written notice of the refusal (s 26WQ(7)).

9.27 Decisions by the Commissioner under s 26WQ are reviewable by the Administrative Appeals Tribunal (AAT).[5] An application for review by the AAT may be made by the entity that made the application for the declaration, or another entity whose obligations under the NDB scheme are affected by the declaration.[6]

Direction of Commissioner — requiring notification (s 26WR)

9.28 The Commissioner may direct an entity to:

- prepare a statement about the eligible data breach
- give a copy of the statement to the Commissioner, and
- notify individuals or CDR consumers about the eligible data breach.

9.29 In deciding whether to give a direction to an entity under s 26WR(1), the Commissioner must consider:

- any relevant advice given to the Commissioner by an enforcement body or the ASD (s 26WR(6)(a))

[5] Privacy Act, ss 96(1)(ba) and 96(bb).

[6] Privacy Act, ss 96(2A) and 96(2B).

- any relevant submission made by the entity (s 26WR(6)(b))
- such other matters (if any) as the Commissioner considers relevant (s 26WR(6)(c)).

9.30 Under s 26WR(5), a direction by the Commissioner may require an entity to include specified information about the eligible data breach, in addition to the information required in a statement prepared for the Commissioner under s 26WR(4).

9.31 The specified information that relates to an eligible data breach is likely to be information that the Commissioner considers would assist individuals or CDR consumers to take appropriate action in response to the eligible data breach. Examples could include:

- information about the risk of harm to individuals that the Commissioner considers exists as a result of the eligible data breach
- recommendations about steps the Commissioner considers individuals should take in response to the eligible data breach
- information about complaint mechanisms available under the Privacy Act to individuals and under the Competition and Consumer Act to CDR consumers who are affected by the eligible data breach
- other specified information relating to the eligible data breach that the Commissioner considers reasonable and appropriate in the circumstances to include in the statement.

Process for making a s 26WR direction

9.32 Before directing an entity to notify, the Commissioner will usually ask the entity to agree to notify voluntarily.

9.33 If the Commissioner and the entity cannot agree about whether notification should occur, the Commissioner will formally invite the entity to make a submission about the direction under consideration, within a specified period (s 26WR(3)). The form of the invitation, and the period of time specified in the invitation for the entity to respond, will be for the Commissioner to determine depending on the particular circumstances. In deciding the form and period of time to respond, the Commissioner will have regard to the impact on the entity and the nature and imminence of the risk of harm to individuals or CDR consumers who would receive notification of the eligible data breach the Commissioner has reasonable grounds to believe has happened.

9.34 The Commissioner will consider submissions and any other relevant information provided by the entity within the period specified before deciding whether to direct the entity to notify under s 26WR.

9.35 The Commissioner's decision will be communicated to the entity in writing. Entities can apply to the AAT for review of a decision by the Commissioner under s 26WR(1) to make a direction.[7]

9.36 An entity must comply with a direction made under s 26WR(1) as soon as practicable (s 26WR(10)). Contravention of s 26WR(10) is an interference with the privacy of an individual (s 13(4A)).

[7] Privacy Act, s 96(1)(bc).

Publication and disclosure of information

9.37 The OAIC will publish statistics in connection with the NDB scheme, with a view to reviewing this approach 12 months after the scheme's commencement.

9.38 The OAIC will respect the confidence of commercially or operationally sensitive information that is provided voluntarily in support of a data breach notification.

9.39 As a matter of course, the Commissioner will consult with entities following a request for information made under FOI law. For FOI requests relating to agencies, the Commissioner will offer to transfer requests to the agency in question.

9.40 Decisions about public communications will be made in accordance with the considerations set out in the 'Public communication as part of privacy regulatory action' section of the *Privacy regulatory action policy,* and where appropriate, the *CDR regulatory action policy*.

Reporting under the My Health Records Act

9.41 Under s 75 of the My Health Records Act, some entities have a mandatory obligation to provide notification of certain data breaches, including potential breaches, in connection with the My Health Record system. The mandatory notification obligation applies to entities that are, or have at any time been, the System Operator,[8] a registered healthcare provider organisation, a registered repository operator, a registered portal operator or a registered contracted service provider (as defined in the My Health Records Act). Depending on the entity involved, notification must be made to either the OAIC or the System Operator or both.

9.42 A failure by a registered healthcare provider organisation, a registered repository operator, a portal operator or a registered contracted service provider to notify in accordance with s 75 is a breach of a civil penalty provision and may result in that entity being liable to pay a penalty.

9.43 The My Health Records Act also outlines in s 75(5) and (6) the steps an entity must take to contain and respond to the breach, or potential breach. The OAIC has developed the *Guide to mandatory data breach notification in the My Health Record system* to assist entities to comply with their mandatory data breach obligations.

9.44 Data breaches that are notified under s 75 of the My Health Records Act*,* do not need to be notified under the NDB scheme.

Responding to data breach notifications under the My Health Records Act

9.45 In assessing and responding to mandatory notifications, the OAIC will consider compliance with the My Health Records Act in addition to compliance with the APPs where relevant. The OAIC may also consider whether the breach was reported 'as soon as practicable', as required under s 75(2).

[8] 'System Operator' is defined in s 14 of the My Health Records Act.

9.46 Section 75(5) of the My Health Records Act requires entities to take certain steps in responding to a data breach that may have occurred or arisen. These steps include containing the breach, evaluating the risks arising from the breach, notifying affected healthcare recipients (if the entity is the System Operator) or asking the System Operator to notify affected healthcare recipients (as applicable). The OAIC will consider these steps when assessing the severity of the breach and the entity's response. Section 75(6) of the My Health Records Act also requires entities to take steps in responding to a data breach that has occurred (rather than to a potential data breach). These steps include containing the breach (and to undertake a preliminary assessment of the causes), evaluating the risks related to or arising from the breach, notifying affected healthcare recipients (if the entity is the System Operator) or asking the System Operator to notify affected healthcare recipients (as applicable) and taking steps to prevent or mitigate the effects of further breaches.

9.47 The Commissioner has investigative powers under s 73(3) of the My Health Records Act, and may use these powers instead of the investigative powers under the Privacy Act if an investigation is warranted following a mandatory notification. However, the Commissioner will generally conduct investigations under the Privacy Act rather than the My Health Records Act unless there is a reason to conduct the investigation under the latter Act.

9.48 When entities are required to notify both the OAIC and the My Health Record System Operator of data breaches, the OAIC may consult with the System Operator when responding to the notification.

Reporting under the National Cancer Screening Register Act

9.49 Under s 22A of the National Cancer Screening Register Act 2016 (NCSR Act), the Secretary of the Department of Health (the Secretary), contracted service providers and former contracted service providers have a mandatory obligation to notify the Information Commissioner of certain data breaches, including potential breaches, in connection with the National Cancer Screening Register.

9.50 A failure by the Secretary, contracted service providers or former contracted service providers to notify in accordance with s 22A is a breach of a civil penalty provision and may result in that entity being liable to pay a penalty.

9.51 The NCSR Act also outlines in ss 22A(4) and (5) the steps the Secretary, contracted service providers or former contracted service providers must take to contain and respond to the breach, or potential breach.

9.52 Data breaches that are notified under s 22A of the NCSR Act, may also need to be notified under the NDB scheme, depending on the circumstances.

9.53 For more information on reporting under the NDB scheme, see paragraph 9.2.

Responding to data breach notifications under the NCSR Act

9.54 The OAIC will generally follow similar steps to the process outlined in relation to the My Health Records Act above [see paragraphs 9.45 to 9.48] when responding to mandatory data breach notifications under s 22A of the NCSR Act.

Reporting under Part VIIIA of the Privacy Act

9.55 Subsection 94S(1) provides that a breach of a requirement under Part VIIIA by the data store administrator (being the administrator, an officer or employee of the administrator, or a contracted service provider under a government contract with the administrator) **is taken to be an eligible data breach** by the data store administrator and the individual to whom the data relates is taken to be at risk from the eligible data breach.

9.56 Subsection 94S(2) provides that a breach of a requirement under Part VIIIA by a State or Territory health authority (being the authority, an employee of the authority or person in the service of the authority) **is taken to be an eligible data breach** by the State or Territory health authority and the individual to whom the data relates is taken to be at risk from the eligible data breach.

9.57 Subsection 94S(3)(a) provides that the breach is an eligible data breach as if the following provisions did not apply:

- S 26WE(3) – this provides that s 26WE(2) (which defines an eligible data breach as an unauthorised access to or disclosure of information that a reasonable person would conclude would be likely to result in serious harm to affected individuals; or that information is lost where unauthorised access is likely to occur and that access would likely result in serious harm to affected individuals) is subject to s 26WF
- S 26WF – a breach is not an eligible data breach if the entity has taken action in relation to the disclosure before any serious harm results and, as a result, the likelihood of serious harm resulting is mitigated
- S 26WH – requirement for an entity to carry out an assessment of whether a breach amounts to an eligible data breach
- S 26WJ – no requirement to conduct an assessment in relation to a breach if another entity has conducted an assessment in relation to the same breach.

9.58 Subsection 94S(3)(c) provides that the breach is an eligible data breach as if the following provisions did not apply:

- S 26WN – exemption from notification of eligible data breach under ss 26WL and 26WK(3)(d) where the chief executive officer of a law enforcement body considers that notification will prejudice enforcement related activities
- S 26WP – exemption from notification of eligible data breach under ss 26WL and 26WK(2)(a)(ii) where compliance would be inconsistent with a secrecy provision
- S 26WQ – exemption from notification of eligible data breach under ss 26WL and 26WK where the Commissioner makes a declaration those provisions do not apply
- S 26WS – exemption from the requirement to comply with a s 26WR(1) direction if the chief executive officer of an enforcement body believes that compliance with the direction is likely to prejudice an enforcement related activity
- S 26WT – exemption from compliance with ss 26WR(1)(b) or 26WR(2) where compliance would be inconsistent with a secrecy provision.

9.59 The effect of these provisions is that any data breach by the data store administrator or a State or Territory health authority **is an eligible data breach, and the entity must comply with the requirements of Part IIIC, regardless of:**

- whether the entity has conducted an assessment and the outcome of that assessment
- whether the entity considers that serious harm is likely to result for affected individuals
- whether the entity has, or has attempted to, mitigate the risk of harm to affected individuals
- whether the entity is an enforcement body and the chief executive officer of that body believes that notification of the eligible data breach would be likely to prejudice one of more enforcement activities they are conducting
- whether there is a secrecy provision (including a prescribed secrecy provision in the regulations) that applies to the information disclosed in the breach
- whether the Commissioner has made a declaration that ss 26WL and 26WK do not apply
- whether the chief executive officer of an enforcement body believes that compliance with a direction of the Commissioner is likely to prejudice an enforcement related activity
- whether compliance with ss 26WR(1)(b) or 26 WR(2) would be inconsistent with a secrecy provision (including a prescribed secrecy provision).

9.60 Further, s 94S(3)(b) requires the data store administrator or State or Territory health authority to:

- notify the Commissioner of the eligible data breach (s 94S(3)(b)(i)) and
- only comply with the following provisions if the Commissioner so requires them to comply:
  - s 26WK – prepare a statement about the eligible data breach and give it to the Commissioner; and
  - s 26 WL – notify affected individuals of the eligible data breach.

9.61 Subsection 94S(4) provides that the Commissioner may consider a range of circumstances when considering whether to require either the data store administrator or State or Territory health authority to prepare a statement about the breach and notify affected individuals (s 94S(3)(b)(ii)), the Commissioner **must** require them to comply with those provisions if both of the following apply:

- the Commissioner is satisfied that the breach may be likely to result in serious harm to any of the individuals to whom the information relates and
- s 94S(5) does not apply.

9.62 Note: the test of 'likely to result in serious harm to any of the individuals' is the same as exists in relation to NDBs notifiable under Part IIIC of the Privacy Act. However, in Part IIIC this assessment is conducted by the notifying entity and is one of the threshold tests for determining whether a data breach is an eligible data breach under those provisions. In relation to COVID app data, this assessment is undertaken by the Commissioner, who must have regard to the outcome of this assessment to comply with s 94S(4).

9.63 Subsection 94S(5) provides guidance for the Commissioner's decision not to require compliance, or extend the period for compliance, with ss 26WK and 26WL. Satisfaction of s 94S(5) also overrides the mandatory requirement for the Commissioner to direct the data store administrator or State or Territory health authority to comply with s 26WK and 26WL

where the Commissioner is satisfied that a breach is likely to result in serious harm to affected individuals.

9.64 Under s 94S(5) the Commissioner may decide not to require compliance, or to extend the period for compliance, if the Commissioner is satisfied on reasonable grounds that it would not be reasonable in the circumstances. In reaching that satisfaction, the Commissioner **must** have regard to:

- the public interest
- relevant advice provided by an enforcement body or the Australian Signals Directorate.

9.65 The Commissioner may take into consideration any other matters as the Commissioner considers relevant or any other advice: s 94S(5)(c) and 95S(6).

9.66 Other than the changes outlined above, the requirements of Part IIIC of the Privacy Act apply.