Data Breach Response Plan

Version 1.1
October 2024

Distribution

Director Professional Standards & Safeguarding	Development and Review	1/10/2021
Professional Standards Advisory Panel	Review and Endorse for Approval	23/11/2021
Provincial Secretary	Review and Endorse for Approval	1/10/2021
Definitory	Review and Endorse	17/12/2021
Provincial Minister	Approval	17/12/2021

Document History

Version	Date	Agent	Approval	Policy Review Due
Version 1.0	17/12/2021	DPSS	ProvMin/Definitory	Dec 2024
Version 1.1	11/10/2024	DPSS	ProvMin/Definitory	

Introduction

1. This Data Breach Response Plan (this Plan) is an internal document outlining the procedures that the Franciscan Friars of the Holy Spirit Province will follow in response to any data breach incident relating to personal information that we hold.
2. Personal information is defined in the *Privacy Act 1988* (Cth) as information or an opinion (whether true or not, and whether or not recorded in material form) about an identified individual, or an individual who is reasonably identifiable.[1]
3. This Plan is intended to be read in conjunction with the Province's ***Privacy Policy,*** which outlines the Province's procedures for collecting, storing, using, disseminating, and disposing of personal information, and which also provides examples of some of the types of personal information the Province may hold.[2]
4. A speedy response to any data breach, based on an up-to-date data breach response plan, is critical for effectively managing any data breach and helping to mitigate potential harm to individuals and organisations. This Plan sets out:
    - the roles and responsibilities of Franciscan Personnel for responding to an actual or suspected data breach;
    - the roles and responsibilities of Franciscan Personnel and contractors/service providers who may have specific responsibilities in the event of an actual or suspected data breach;
    - procedures to be followed for containing, assessing, and reporting an actual or suspected data breach.
5. This Plan has been approved by the Provincial Minister and his Definitory acting also in their capacity as directors of Franciscan Order of Friars Minor, which is the corporate entity associated with the Province in Australia. The Province Administration will review the Plan at least once every three years, or as required by legislative changes.

1 See *Privacy Act 1988* (Cth), s 6(1).

2 See ***Privacy Policy,*** para 22.

Application of this Plan

6. This Plan applies to any actual or suspected data breach incident involving personal information held by the Province, or by the Province's corporate civil entity in Australia, the Franciscan Order of Friars Minor.[3] (Hereafter, references to the Province include the Franciscan Order of Friars Minor.)
7. This Policy does not apply to the Friars Minor of New Zealand Trust Board (FMNZTB), or its employees or volunteers. As the separately constituted Franciscan corporate civil entity in Aotearoa-New Zealand, the FMNZTB is responsible for developing its own polices and procedures, specific to its own operation.

3 Personal information that is "held by" the Province includes personal information that is in the possession or under the control of the Province.

Relevant laws

8. Because the Province's central administration is located in Australia, and the Franciscan Order of Friars Minor is incorporated in Australia, we adhere to the *Privacy Act 1988* (Cth) (the Privacy Act) and the Australian Privacy Principles, which regulate the collection, use, and disclosure of personal information.
9. Where they apply to our operations or activities in Aotearoa-New Zealand, we adhere to the *Privacy Act 2020* (NZ).
10. In some circumstances, privacy laws may have extraterritorial application – that is, a country's privacy law provisions may apply to entities which are registered or located, or to conduct which takes place, outside that country. The Province adheres to extraterritorial laws where they apply to our operations or activities and where doing so will not cause us to contravene applicable local laws.
11. This Plan has been developed with guidance from the Office of the Australian Information Commissioner for management of data breaches in accordance with Australia's Privacy Act.[4] Because the Province operates in and across different countries, in some cases we may be subject to different requirements for data breach responses under the privacy laws of other jurisdictions.[5] In such cases, we will comply with the requirements of applicable laws, and we will adhere to this Plan to the extent that doing so does not contravene an applicable law.[6]
12. This Plan is not intended to direct Franciscan Personnel to act in contravention of any laws that apply to the handling of personal information in particular cases. In any circumstances where compliance with this Plan would result in a breach of applicable law, Franciscan Personnel are to comply with the applicable law.

4 OAIC, *Data Breach Preparation and Response: A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth),* July 2019.

5 The Province's transnational territory includes Australia and Aotearoa-New Zealand, and the international headquarters of the Order of Friars Minor is based in Rome. Consequently, as well as handling of personal information within different jurisdictions, there may be occasions when we need to transfer personal information across national borders for the purposes of undertaking and administering our ministries, functions and activities, and otherwise when we are legally required to do so. We are committed to maintaining the protection of personal information we transfer to overseas recipients and will comply with our obligations, under applicable law and our ***Privacy Policy,*** in this respect.

6 There are, for example, some differences under the privacy laws of Australia and New Zealand. See Part 6 of the *Privacy Act 2020* (New Zealand) for provisions setting out data breach assessment and notification requirements in New Zealand.

What is a data breach?

13. In the context of the Privacy Act, a data breach occurs when personal information held by the Province is the subject of unauthorised access, disclosure, use, modification or other misuse, or is lost, whether accidentally or intentionally.[7]

14. Data breaches can take many different forms. Examples of the types of data breach that might potentially affect personal information held by the Province, include but are not limited to:

    - loss or theft of physical devices such as laptops, mobile phones, or storage devices containing personal information;
    - a computer hacking incident involving unauthorised access to or control over the Province's email system or the digital files stored on the Province's online server;
    - loss or theft of paper records held at the Provincial Office;
    - unauthorised access to or disclosure of personal information by Franciscan Personnel;
    - inadvertent disclosure of personal information through "human error" – for example, an email sent to the wrong addressee;
    - disclosure of personal information to a scammer, as a result of inadequate identity verification procedures.

15. In Australia, the Province has specific obligations under the Privacy Act in respect of personal information that we hold.[8] The Province must:

    - take reasonable steps to protect any personal information it holds from unauthorised access, misuse, interference, modification, disclosure, or loss;[9]

7 See *Privacy Act 1988* (Cth), Part IIIC and *Privacy Act 2020* (NZ), Part 6 for what constitutes a data breach under those laws.

8 Entities with obligations under the Privacy Act include Australian Government agencies, businesses and non-for-profit organisations with an annual turnover of more than $3 million, private sector health service providers, credit reporting bodies, credit providers, entities that trade in personal information, and tax file number (TFN) recipients in relation to their handling of TFN information.

9 See *Privacy Act 1988* (Cth), Schedule 1, Australian Privacy Principles, 11.1. The Province takes all reasonable steps to protect and secure the personal information we hold from unauthorised access, disclosure or modification, or other misuse, interference or loss. These steps include restricted access to Provincial offices and other areas where personal information is stores, password-protected computer files that can be accessed only be authorised individuals, the use of high-security IT systems, and the provision of regular training to all Franciscan personnel about the importance of maintaining the confidentiality and security of personal information.

What is a data breach? (Cont'd)

- have procedures in place to contain, assess, and respond to an actual or suspected data breach incident in a timely manner;[10]
- where necessary, notify affected individuals and the Australian Information Commissioner (the Commissioner) about "eligible data breaches".[11]

16. An "eligible data breach" is a data breach that meets the following criteria:
    - there are reasonable grounds to believe there has been unauthorised access to, unauthorised disclosure of, or loss of personal information held by the Province;
    - as a result, there is a likely risk of serious harm to any of individual or individuals to whom the personal information relates;[12] and
    - the Province has been unable to prevent the likely risk of serious harm with remedial action.
17. Procedures for notifying affected individuals and the Commissioner about an eligible data breach relating to personal information held by the Province in Australia are outlined below.
18. It is important to note that the Privacy Act and the Office of the Australian Information Commissioner (OAIC) are only concerned with breaches that involve personal information. Data breaches that do not involve personal information do not have to be reported to the Commissioner. However, the procedures set out in this Plan can also assist with responding to actual or suspected data breaches that do not involve personal information.

10 See *Privacy Act 1988* (Cth), s 26WH.

11 See *Privacy Act 1988* (Cth), Part IIIC.

12 A determination needs to be made about whether, from the perspective of a reasonable person, the data breach would be likely to cause serious harm to any person or persons whose personal information is affected by the data breach. "Serious harm" is not defined in the Privacy Act, but in this context it could mean serious physical, psychological, emotional, economic, financial, reputational, or other forms of serious harm that a reasonable person would identify as a possible outcome of a data breach. It could include identity theft; significant financial loss; threats to a person's physical safety; loss of business or employment opportunities; humiliation or damage to a person's reputation or relationships; workplace or social bullying or marginalisation.

What is a data breach? (Cont'd)

19. The OAIC is able to further provide information and advice about what constitutes an eligible data breach and the steps that organisations need to be take in response to an eligible data breach.[13] The OAIC can be contacted on 1300 363 992 between 10.00 am and 4.00 pm, Mon-Thurs AEST/AEDT or via an online inquiry form which is available here: https://www.oaic.gov.au/contact-us

20. In the event of an actual or suspected data breach incident involving personal information that the Province holds or handles in Aotearoa-New Zealand,[14] different assessment and notification obligations may apply. As stated above, in such cases we will comply with the requirements of applicable laws, and we will adhere to this Plan to the extent that doing so does not contravene any applicable law.

13 This Plan draws heavily on the OAIC's Data Breach Preparation and Response: A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth), July 2019.

14 For provisions covering assessment and notification of data breaches involving personal information in New Zealand, see the *Privacy Act 2020*, Part 6 – notification is to the Privacy Commissioner.

Data Breach Response Team:

21. The members of the Province's Data Breach Response Team are as follows:

Data Breach Response Team
Provincial Secretary (Team Leader)
Administrative Officer (Project Support)
As required (depending on whether their area of operation is affected):
Archivist
Director, Professional Standards and Safeguarding
Director of Finance
Provincial Delegate for the Region of St Andrew (Aotearoa-New Zealand)
External expertise (as required):
IT support (Claratti Ltd)
Legal support
Media/Communications support

Procedures for responding to actual or suspected data breach incidents

22. The Provincial Secretary will take the lead in co-ordinating the Province's response to any data breach incident.

23. Any Franciscan Personnel who become aware of an actual or suspected data breach must immediately notify the Provincial Secretary of the time and date when the incident was detected, and (if known) the time or date range when the incident occurred, the type of personal information involved, and the cause of the actual or suspected breach. The Provincial Secretary may be contacted by telephone at **+61 2 9369 9302**, or by email at provsec@franciscans.org.au.

24. Data breaches can be caused or exacerbated by a variety of factors, affect different types of personal information, and give rise to a range of actual or potential harms to individuals and organisations depending on the situation. For this reason, how best to respond to any specific data breach will need to be determined on a case-by case basis. However, all data breaches should be treated seriously and immediately acted upon.

25. In general, the actions taken following a data breach should follow four key steps:

    Step 1: Contain the actual or suspected data breach to prevent any further compromise of personal information.

    Step 2: Assess the risk of potential harm to affected individuals or organisations, taking appropriate remedial action where possible.

    Step 3: Notify affected individuals and the Commissioner if required.

    Step 4: Review the incident and consider what action if any needs to be taken to prevent further breaches.

Step 1: Contain

26. If the Provincial Secretary is notified, or becomes aware, that a data breach has been discovered or is suspected to have occurred, immediate steps should be taken to contain the breach and reduce any potential harm to individuals or organisations where possible. For example, this could mean stopping an unauthorised practice, taking steps to recover lost records or devices, shutting down the system that was breached, or changing passwords or access privileges.

27. Addressing the following questions may help to identify strategies to contain a data breach:

    - How did the data breach occur?
    - Is confidential information or personal information still being shared, disclosed, or lost without authorisation?
    - Who has access to the confidential information or personal information?
    - What can be done to secure the information, or stop the unauthorised access or disclosure, and reduce the risk of harm to affected individuals or organisations?

28. In the event of an actual or suspected IT breach, the Provincial Secretary will immediately notify the Province's IT service provider, Claratti, for assistance on **1300 005 969.**

29. In the event that Claratti is the first to discover or be made aware of an actual or suspected data breach, Claratti will immediately notify the Provincial Secretary.

30. Claratti has its own Information Security Incident Response Procedure in place, and this Plan is intended to operate in conjunction with it. In the event of an actual or suspected IT breach, Claratti will be able to take immediate containment action, undertake its own forensic assessment of when, how and why a data breach incident occurred, and report back to the Provincial Secretary. If Claratti considers that it does not have the internal expertise to deal with a particular incident, it will be able to provide advice about any outside IT expertise that might be needed.[15]

15 It should be noted that under the Privacy Act, where the Province stores personal information contained in records with a cloud service provider, the cloud service provider is taken to "hold" the information. However because the Province retains legal control or ownership over the records, both entities are taken to "hold" the information. In these circumstances, an eligible data breach of one entity will also be considered an eligible data breach of the other entity that holds the information. Both entities will have obligations under the Privacy Act, but in general, compliance by one of the entities with its assessment and notification obligations under the Privacy Act will be taken as compliance by both. The OAIC suggests that, in general, the entity with the most direct relationship with individuals whose personal information is affected by the data breach should carry out notification.

Step 1: Contain (Cont'd)

31. It is important that accurate records are made of any actions taken and/or evidence gathered throughout the entire process of responding to any data breach. These records may be required as part of any resulting investigations by relevant regulatory or law enforcement agencies.
32. Care needs to be taken not to destroy evidence that might be valuable in identifying the cause or source of the breach, or that would enable the Province to address all risks posed to affected individuals or organisations. Particularly where digital evidence may need to be collected that will later be used in court, precaution must be taken to ensure that such evidence remains admissible. This means that relevant data must not be deliberately or accidentally changed.
33. If the Provincial Secretary or Claratti suspect or believe that a serious crime is likely to have occurred or is occurring, a report must be made to the police as soon as is practicable. Where a matter has been reported to the police because it involves criminal conduct, the Provincial Secretary must consult with police before taking any steps that might compromise a police investigation. Agreement should be sought from police about any immediate steps that need to be taken to manage any risk of harm to affected individuals or any internal risks.

Step 2: Assess

34. When notified of an actual or suspected data breach incident, the Provincial Secretary will carry out a prompt preliminary assessment to determine:
    - whether an actual data breach has occurred;
    - the scale of the incident;
    - whether there is a risk of serious harm to any affected person or organisation that would require the convening the Data Breach Response Team.
35. During this preliminary assessment stage, basic information about the incident should be collected, including a chronology of the incident, details of any witnesses, photographs or videos of any relevant messages or information, and any relevant original documents, including records of who found them, where, and when.
36. In making a preliminary assessment about whether there is a risk of serious harm to any person whose personal information is affected by the data breach, the Provincial Secretary will need to consider:
    - the type or types of person information;[16]
    - the sensitivity of the personal information;[17]
    - whether the personal information is protected by one or more security measures, and if so, the likelihood that those security measures have been or could be overcome;
    - the persons, or types of persons, who have obtained, or who could obtain, the personal information, including whether they have, or are likely to have, the intention of causing harm to any of the individuals to whom the personal information relates;
    - the nature of the harm;
    - any other relevant matters.[18]

16 Types of information that may be more likely to cause an individual serious harm if there were a data breach include "sensitive information" such as information about a person's health status; documents commonly used in identity fraud such as passports, driver's licence, and Medicare card; financial information; or a combination of types of personal information relating to any one person.

17 The Province's ***Privacy Policy*** **[link]** defines "sensitive information" in line with the Privacy Act as "information or an opinion (whether true or not) about a person's racial or ethnic origin, political beliefs, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association or trade union, sexual orientation or practices, criminal record, health information, genetic information, or biometric information."

18 Privacy Act, s 26WG.

Step 2: Assess (Cont'd)

37. If the Provincial Secretary's preliminary assessment is that the data breach is a minor incident which can be dealt with by the Provincial Secretary alone, or with limited assistance (for example, assistance from Claratti), the following details should be recorded:

    - description of the breach or suspected breach;
    - action taken by the Provincial Secretary and/or Claratti;
    - outcome of that action.

38. The Provincial Secretary should immediately convene the Data Response Team if any of the following factors apply:

    - the actual or suspected data breach is not a minor incident that can easily be resolved;
    - the actual or suspected data breach is significant or has the potential to be significant (for example, it may affect or have the potential to affect a significant number of people);
    - there is a risk of serious harm to any individual whose personal information is affected by the actual or suspected data breach;
    - the actual or suspected data breach:
        - o gives rise to obligations for response under the laws of jurisdictions other than Australia, or
        - o involves the transfer of personal information across national borders, or
        - o may be in breach of privacy laws which may have extraterritorial application;[19]
    - the actual or suspected data breach is indicative of a systemic problem in the Province's processes for protecting personal information;
    - the actual or suspected data breach has caused, or has the potential to cause, significant disruption to the Province's operations;
    - the actual or suspected data breach has the potential to cause reputational risk;
    - there is a potential for m edia or stakeholder attention as the result of the actual or suspected data breach.

19 Where the data breach involves the transfer of personal information across national borders, it may be necessary to seek advice from/notify the Australian Federal Police and/or the privacy regulation agency in the relevant country. It may also be necessary to obtain specialist legal advice about applicable privacy law in that country. It should be noted that when an Australian entity with obligations under the Privacy Act discloses personal information to an overseas recipient, the Australian entity is still deemed to be "holding" the personal information if it is subject to unauthorised access, disclosure or loss. This means the Australian entity is still responsible for assessing whether there has been an "eligible data breach" and notifying affected individuals and the Commissioner (see Privacy Act, s 26WC).

Step 2: Assess (Cont'd)

39. The primary role of the Data Breach Response Team is to make an assessment based on all the available information about whether there are reasonable grounds to believe that an "eligible data breach" has occurred.[20] This assessment should be completed as quickly as is possible in order to mitigate any potential harm to affected individuals or organisations. In making its assessment, the Data Breach Response Team will need to:
    - clearly establish what personal information was involved in the data breach;[21]
    - develop as full an understanding of the potential impact of the data breach as possible;
    - consider whether any further legal or specialist advice is needed.[22]
40. Where possible, the Data Breach Response Team will seek to identify any individuals whose personal information has been affected and who are at risk of serious harm due to the data breach. If practicable, their contact details should be assembled in case they need to be notified.[23]

20 Under the Privacy Act, the requirement for an assessment is triggered if the organisation has reasonable grounds to suspect that there may have been an eligible data breach. See s 26WH.

21 Sensitive Information means information or an opinion (whether true or not) about a person's racial or ethnic origin, political beliefs, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association or trade union, sexual orientation or practices, criminal record, health information, genetic information, or biometric information.

22 Examples of possible sources of advice in relation to data breaches within Australia include but are not limited to:

- the Commissioner;
- Federal, State or Territory police;
- the Province's financial services provider;
- the Province's online (cloud storage) service provider;
- the Province's insurance provider;
- the Australian Taxation Office (ATO);
- the National Redress Scheme (NRS);
- Computer Emergency Response Team Australia (CERT);
- Australian Cyber Security Centre (ACSC);
- Australian Transaction Reports and Analysis Centre (AUSTRAC);
- Australian Digital Health Agency (ADHA);
- State or Territory Privacy and Information Commissioners

23 Where there are reasonable grounds for believing that an individual or individuals are at risk of serious harm due to a data breach, steps should be taken to notify them as expeditiously as possible. This step does not need to wait until a statement for the Commissioner has been prepared. However, any such notification is a sensitive issue that must be handled carefully and with the approval of the Provincial Secretary. Notification of affected individuals can sometimes cause undue stress or harm. In deciding whether or not to notify affected individuals, caution should be exercised so that individuals are not notified in circumstances where it is inappropriate or unnecessary to do so. Each incident needs to be considered on a case-by-case basis.

Step 2: Assess (Cont'd)

41. Where an assessment is made that an "eligible data breach" has occurred, drawing on all the available information and any legal or other specialist advice that is required, the Data Breach Response Team will:

    - prepare a statement for the Commissioner (see paragraphs 37-39, below);
    - decide how the notification of affected individuals should occur, including what information is to be provided in the notification,[24] what form the notification will take, and who will have responsibility for making the notification (see paragraphs 40-43, below);
    - consider whether any applicable law requires any other regulatory or law enforcement agency to be notified,[25] and whether any banking, financial services, insurance, or other service provider should be notified;
    - consider whether a media and communications strategy needs to be developed.

24 Decisions about what information is to be provided will depend on the circumstances, but, generally speaking, the notification to affected individuals should include the information set out at paragraph 36. The Data Breach Response Team will consider whether any other requirements apply pursuant to the privacy laws of jurisdictions other than Australia, and seek specialist advice where necessary to ensure any notifications made are adequate and lawful.

25 For example, Federal, State, or Territory police, or (for a data breach involving tax file numbers) the ATO, or (for a data breach involving information protected under Australia's National Redress Scheme) the NRS.

Step 3: Notify

42. If the Data Breach Response Team makes a determination that there are reasonable grounds for believing that there has been an eligible data breach, a statement must be prepared and sent to the Commissioner as soon as is practicable, setting out:
    - the Province's name, address, and contact details;
    - a description of the eligible data breach that the Province has reasonable grounds to believe has occurred;[26]
    - the types of personal information involved;
    - recommendations directed to affected individuals about the steps they should take in response to the eligible data breach in order to mitigate serious harm or the likelihood of serious harm.[27]
43. The OAIC has provided an online form for organisations reporting an eligible data breach, which is available here: https://webform.oaic.gov.au/prod?entitytype=DBN&layoutcode=DataBreachWF
44. If the Data Breach Response Team has reasonable grounds for believing that the eligible data breach is also an eligible data breach for more than one entity, the statement may also set out the identities and contact details for that other entity or entities.[28]
45. In response to being notified, the Commissioner may seek further information or provide advice and guidance about how the Province should assist individuals at risk of serious harm. The Commissioner also has certain enforcement powers in relation to breaches of privacy. For example, in certain circumstances the Commissioner can direct an entity to notify individuals at risk of serious harm. In exceptional circumstances, the Commissioner may make a declaration that notification of a particular data breach is not required.[29]

26 This description should include the date or date range when the eligible data breach occurred, the date when the Province detected the data breach, the circumstances of the data breach (such as any known causes for the unauthorised access, disclosure or loss of the affected information), who has obtained or is likely to obtain access to the information, and any relevant information about what steps the Province has taken to contain or remediate the breach.

27 This may entail recommending steps that are tailored to a particular affected individual's circumstances, or providing general recommendations that apply to all affected individuals. For example, it may be recommended that affected individuals monitor their bank accounts and immediately report any suspicious activity to their bank, or contact their bank to put a hold on their credit card or change their credit card number. Where the Province does not have the knowledge or capacity to provide advice to affected individuals, specialist advice should be sought in preparing this section.

28 Where more than one entity holds personal information that is compromised by an eligible data breach, only one entity is required to prepare a statement for the Commissioner and notify affected individuals.

29 In order to make such a declaration, the Commissioner needs to be satisfied that it is reasonable in the circumstances to do so, having regard to the public interest, any relevant advice received from an enforcement body or the Australian Signals Directorate, and any other relevant matter.

Step 3: Notify (Cont'd)

46. As well as notifying the Commissioner, the Province is required, if it is practicable to do so,[30] to notify each individual whose personal information has been affected by the eligible data breach, or each individual who is at risk of serious harm due to the eligible data breach, about the content of the statement prepared for the Commissioner.[31] Any notification method may be used, including telephone, SMS, postal mail, email, social media post, or in-person conversation.

47. If the Province is able to identify that a particular individual or an identifiable subset of individuals is at risk of serious harm due to eligible data breach, only those individuals are required to be notified. This kind of targeted approach will avoid causing unnecessary alarm or distress to those who are not at risk of serious harm. In notifying individuals, care must be taken not to disclose any personal information that does not belong to those individuals.[32]

48. It is important that Franciscan Personnel who have the task of notifying and engaging with affected individuals do so with sensitivity and compassion in order not to exacerbate or cause further harm. Where the Data Breach Response Team is concerned that notifying an affected individual or individuals has the potential to cause further harm, advice should be sought from the OAIC.

49. If it is not practicable to directly notify each of the affected individuals of the content of the statement prepared for the Commissioner, the Province is required to publish the statement on its website, and take any further reasonable steps to make affected individuals aware of the statement.[33] If this is the notification option that is chosen, care must be taken that the published statement does not contain any personal information.[34]

50. If required, other law enforcement or regulatory agencies, and/or financial, insurance or other relevant organisations should be notified.

30 In deciding whether or not it is "practicable" to notify each individual directly, consideration should be given to the time, effort, and cost involved.

31 Where the Province has already notified affected individuals about the data breach prior to notifying the Commissioner, they do not need to notify those individuals again, as long as the individuals were notified of the information contained in the contents of the statement provided to the Commissioner.

32 See Privacy Act, s 26WL.

33 For example, by taking out an advertisement in a newspaper. In general, the seriousness of the actual or potential harm and the number of individuals affected will have a bearing on whether it would be reasonable to take any such further steps.

34 See Privacy Act, s 26WL.

Step 4: Review

51. Following the conclusion of a serious data breach incident, the Data Breach Response Team must review the incident to consider:
    - what underlying factors may have contributed to the data breach;
    - what further safeguards, policies or practices could be put into place to prevent or reduce the risk of similar incidents in the future; and
    - any systemic issues that have emerged in relation recruitment, screening, training or supervision of Franciscan Personnel that may require attention by the Provincial Minister.
52. If the data breach incident involved an IT breach, Claratti will be able to assist with any review of the incident.
53. The Data Breach Response Team must report on the outcome of the review to the Provincial Minister, who will bring the review to the attention of the Definitory and, where relevant, to the attention of all Franciscan Personnel and will take action as appropriate in response to the review.
54. Following a minor data breach which has been resolved internally or with the assistance of Claratti, the Provincial Secretary will review the incident. The Provincial Minister and Definitory should be informed about even minor data breaches.
55. The Data Breach Response Team must report on the outcome of the review to the Provincial Minister, who will bring the review to the attention of the Definitory and, where relevant, to the attention of all Franciscan Personnel and will take action as appropriate in response to the review.

Data Response Flow Chart

Actual or suspected data breach discovered by Franciscan personnel

- Immediately inform Provincial Secretary of the suspected data breach, including the time when the discovery was made and (if known) the cause and the type of personal information involved.

Step 1: Contain

Provincial Secretary takes lead in Province's response to the incident

- Provincial Secretary immediately conducts a preliminary assessment of whether an actual data breach has occurred, its scale and seriousness, and takes steps to contain the breach.
- If the incident is minor and able to be contained, the Provincial Secretary documents the incident and action taken and makes an incident report to Provincial Minister and Definitory.
- If the incident involves an IT breach, Provincial Secretary immediately contacts Claratti.
- If it is suspected that a serious crime has occurred or is occurring, the Provincial Secretary contacts the police.
- If the incident is serious and/or the Provincial Secretary is unable to contain it, the Provincial Secretary immediately convenes the Data Breach Response Team

Step 2: Assess

Assessment by Data Breach Response TeamProvincial Secretary

Data Breach Response Team assesses:

- whether there are reasonable grounds for believing that an "eligible data breach" has occurred
- what information is involved, and attempts to identify individuals whose personal information is affected or who are at risk of serious harm due to the breach;
- whether any further required legal or other specialist advice.

If there are reasonable grounds for believing that an eligible data breach has occurred, the Data Breach Response Team:

- prepares a statement for the Commissioner;
- decides how affected individuals should be notified occur, including the form of notification, what information is to be provided, and who will have responsibility for making the notification;
- consider whether any other regulatory or law enforcement agency or any banking, financial services, insurance, or other provider should also be notified;
- consider whether a media and communications strategy needs to be developed.

Data Response Flow Chart

Step 3: Notify

Who must be notified in the event of an eligible data breach?

- A statement must be sent to the Commissioner, including a description of the breach, the type of personal information involved, and recommendations directed to affected individuals about steps they should take to mitigate serious harm or the likelihood of serious harm.
- If practicable, any individuals whose personal information has been affected, or who are likely to suffer serious harm, should be notified.
- If it is not practicable to directly notify each of the affected individuals, the Province is required to publish the statement on its website, and take any further reasonable steps to make affected individuals aware of the statement.
- Where required, other law enforcement or regulatory agencies, and/or financial, insurance or other relevant organisations should also be notified.

Step 4: Review

Assessment by Data Breach Response TeamProvincial Secretary

- Minor incidents are reviewed by Provincial Secretary who reports to Provincial Minister and Definitory with recommendations for any necessary changes to policies or practices.
- Serious incidents are reviewed by Data Breach Response Team which reports to Provincial Minister and Definitory with recommendations for any necessary changes to policies or practices

Definitions

Commissioner:

Means the Australian Information Commissioner (OAIC).

Confidential Information:

means information that is controlled and only available on a need to know basis in order for employees to perform their duties.

Data Breach:

means an incident where personal information held by the Province is the subject of unauthorised access, disclosure, use, modification or other misuse, or is lost, whether accidentally or intentionally.

Data Breach Response Team:

means the team that may need to be convened by the Provincial Secretary to provide advice and/or assist in responding to a data breach.

Eligible data breach:

means a data breach which meets the following criteria:

- there are reasonable grounds to believe there has been unauthorised access to, unauthorised disclosure of, or loss of personal information held by the Province;
- as a result, there is a likely risk of serious harm to any of individual or individuals to whom the personal information relates; and
- the Province has been unable to prevent the likely risk of serious harm with remedial action.

Franciscan Personnel:

means all friars and all Franciscan employees and volunteers appointed to any position administered by the Franciscan Holy Spirit Province or by the Province's corporate civil entity in Australia, the Franciscan Order of Friars Minor.

IT breach:

means a breach involving the Province's computer system or email system, including records stored in the cloud by the Province's IT service provider, or devices such as computers, laptops, mobile phones or any other digital storage device.

Personal information:

means information or an opinion (whether true or not, and whether or not recorded in material form) about an identified individual, or from which an individual's identity can reasonably be determined.[35]

35 Personal information is defined under Australian law as information or an opinion (whether true or not, and whether or not recorded in material form) about an identified individual, or an individual who is reasonably identifiable. See *Privacy Act 1988* (Cth), s 6(1). This definition is largely consistent with the characterisation of personal information in other jurisdictions in the Province. Under New Zealand law, 'personal information' means information about an identifiable individual: *Privacy Act 2020* (NZ), s7(1).

Definitions (Cont'd)

Sensitive information

means information or an opinion (whether true or not) about a person's racial or ethnic origin, political beliefs, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association or trade union, sexual orientation or practices, criminal record, health information, genetic information, or biometric information.

Serious harm:

means serious physical, psychological, emotional, economic, financial, reputational, or other forms of serious harm that a reasonable person would identify as a possible outcome of a data breach. It could include identity theft; significant financial loss; threats to a person's physical safety; loss of business or employment opportunities; humiliation or damage to a person's reputation or relationships; workplace or social bullying or marginalisation.
oluntary basis.

Contact:

Franciscan Provincial Office
Franciscan Friars | Holy Spirit Province
47 Victoria Street | Waverley NSW 2024 | Australia
p: +61-2-9369 9300 or 1800 411 610
e: profstand@franciscans.org.au | www.franciscans.org.au