Australian Government

Office of the Australian Information Commissioner

COVIDSafe Assessment 3: COVIDSafe application functionality, privacy policy and collection notices

Privacy Assessment by the Office of the Australian Information Commissioner

30 September 2021

Contents

COVIDSafe Assessment 3: COVIDSafe application functionality, privacy policy and collection notices

Part 1: Executive summary

1.1 This report outlines the findings of the Office of the Australian Information Commissioner's (OAIC) privacy assessment of the Australian Government's COVIDSafe application (COVIDSafe app), the APP Privacy Policy (COVIDSafe Privacy Policy) and collection notices for the COVIDSafe app, conducted from November 2020 to January 2021.

1.2 This assessment was conducted under s 33C(1)(a) of the *Privacy Act 1988* (Cth) (Privacy Act), which allows the OAIC to assess whether an entity maintains and handles the personal information it holds in accordance with the Australian Privacy Principles (APPs).

1.3 This assessment was also conducted under s 94T(1) of the Privacy Act, which extends s 33C to allow the OAIC to assess whether the acts or practices of an entity or a State or Territory authority in relation to COVID app data comply with Part VIIIA of that Act.

1.4 The purpose of this assessment was to determine whether:

- the COVIDSafe Privacy Policy and collection notices meet the requirements of APPs 1.3, 1.4, and APP 5
- the design and technical implementation of the COVIDSafe app, the Health Official Portal (HOP) and the National COVIDSafe Data Store (NCDS)) (together, the COVIDSafe System) aligns to the COVIDSafe Privacy Policy, collection notices and recommendations outlined in the COVIDSafe application Privacy Impact Assessment (PIA)[1]
- the COVIDSafe System complies with the collection, use, disclosure and retention requirements of Part VIIIA of the Privacy Act.

1.5 The scope of the assessment was expanded to include consideration of APP 1.5.

1.6 This privacy assessment found that the Australian Government, represented by the Australian Government Department of Health (DoH) and the Digital Transformation Agency (DTA):

- has a clearly expressed and up to date privacy policy for the COVIDSafe app that meets the requirements of APP 1.3 and 1.4
- is taking reasonable steps to inform COVIDSafe users of the collection of COVID app data at the time of collection via a collection notice that complies with the requirements of APP 5.

[1] COVIDSafe application PIA conducted by Maddocks dated 24 April 2020.

1.7 However, this assessment identified 2 medium privacy risks in relation to the need for an appropriate collection notice available at or before the time of collection of personal information via the 'Request data deletion' Webform on the COVIDSafe website that notifies or ensures awareness of individuals of the APP 5 matters in accordance with the requirements of APPs 5.1 and 5.2.

1.8 The assessment also identified 6 low privacy risks associated with the COVIDSafe Privacy Policy and collection notice relating to:

- providing COVIDSafe users an explanation of how the encrypted user ID is created and assigned to each user
- advising COVIDSafe users in the COVIDSafe Privacy Policy that access to their COVID app data is not permitted by law
- the use of inconsistent terminology in the COVIDSafe Privacy Policy and collection notices to refer to the collection of a certain type of personal information
- the COVIDSafe app collection notices not including information regarding:
  - the identity and contact information of the APP entity collecting the personal information
  - the fact that the collection of personal information is authorised by the Privacy Act
  - an explicit statement regarding the consequences in the event an individual does not provide their personal information.

1.9 The OAIC has made 2 recommendations and 6 suggestions in the report to address these privacy risks. The recommendations, suggestions, and the DTA's responses, are outlined in Part 3 and Part 4 of this report.

Part 2: Introduction

Background

The COVIDSafe System

2.1 The COVIDSafe System refers to the system comprising the COVIDSafe app, the NCDS, the HOP and the technological, administrative and legal measures which ensure the effective operation of the system and its compliance with applicable legislation.

2.2 The COVIDSafe System has been described in detail in COVIDSafe Assessment 1: National COVIDSafe Data Store Access Controls (COVIDSafe Assessment 1). As such, only a brief description of the COVIDSafe app, NCDS and the HOP is provided here. Please refer to this assessment report for further background information on the COVIDSafe System.

COVIDSafe app

2.3 The COVIDSafe app is a voluntary contact tracing mobile application developed by the DTA to help identify close contacts of COVID-19 cases, and to help State and Territory health officials (STHA officials) contact people who may have been exposed to COVID-19. The COVIDSafe app is available on both iOS and Android communication devices. The COVIDSafe app exchanges a 'digital handshake', via Bluetooth, between COVIDSafe users who are within 1.5 metres of each other.

National COVIDSafe Data Store (NCDS)

2.4 The NCDS is a cloud-based storage solution for information collected or generated using the COVIDSafe app. The NCDS is maintained by the DTA as the Data Store Administrator (DSA) and is hosted by Amazon Web Services (AWS). Registration Data[2] entered by COVIDSafe users is encrypted and stored in the NCDS. Digital handshakes may be uploaded to the NCDS, following a COVIDSafe user testing positive for COVID-19 and consenting to upload the data via the COVIDSafe app to the NCDS.

Health Official Portal (HOP)

2.5 The HOP is an online portal for State or Territory health authorities (STHA) to access COVID app data stored within the NCDS. The HOP allows STHA officials to:

- access Registration Data (via a phone number search)
- request a COVIDSafe user to upload their Bluetooth 'digital handshakes' following a

[2] Registration Data is defined at para 2.13.

positive diagnosis for COVID-19

- filter the Bluetooth 'digital handshakes', via date range and proximity probability, to identify potential close contacts of a COVIDSafe user who has received a positive diagnosis for COVID-19.

2.6 The HOP defines a 'close contact' as 2 or more COVIDSafe users whose devices are within 1.5 metres consistently for 15 minutes. It categorises these close contacts as either stable (where contact is maintained every minute for the 15 minute period), or sporadic (where contact over a 15 minute period is intermittent).

COVID app data lifecycle

2.7 'COVID app data' is defined in s 94D(5) of the Privacy Act as data relating to a person that:

a. has been collected or generated through the operation of the COVIDSafe app, and

b. either is Registration Data, or is stored, or has been stored, on a communication device.

2.8 The flow of COVID app data through the COVIDSafe System, the points at which collection notices are provided to COVIDSafe users and consent is sought by the DTA is depicted in figure 1.

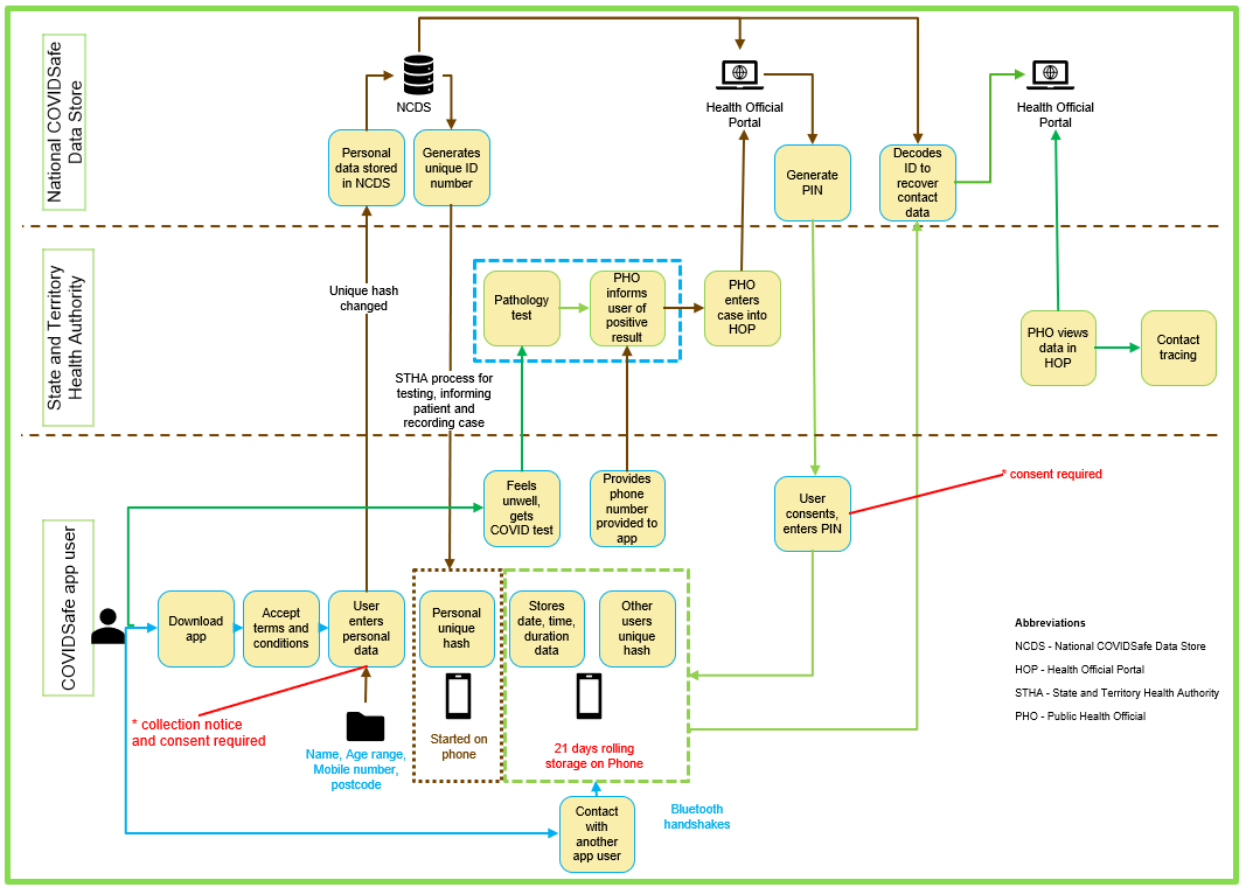


Figure 1: The flow of personal information through the COVIDSafe System, and points at which collection notices are provided and consent is sought by the DTA.

Collection

2.9 COVID app data is only collected via the COVIDSafe app. During fieldwork the OAIC observed that when a user downloads the COVIDSafe app, at the commencement of the app set up process they are provided with initial information on the purpose and function of the COVIDSafe app (see figure 2). Under the heading 'How COVIDSafe works' there is a link to the help topics (highlighted by the red box in figure 2) that provides additional information on the COVIDSafe app and a link to the COVIDSafe Privacy Policy.

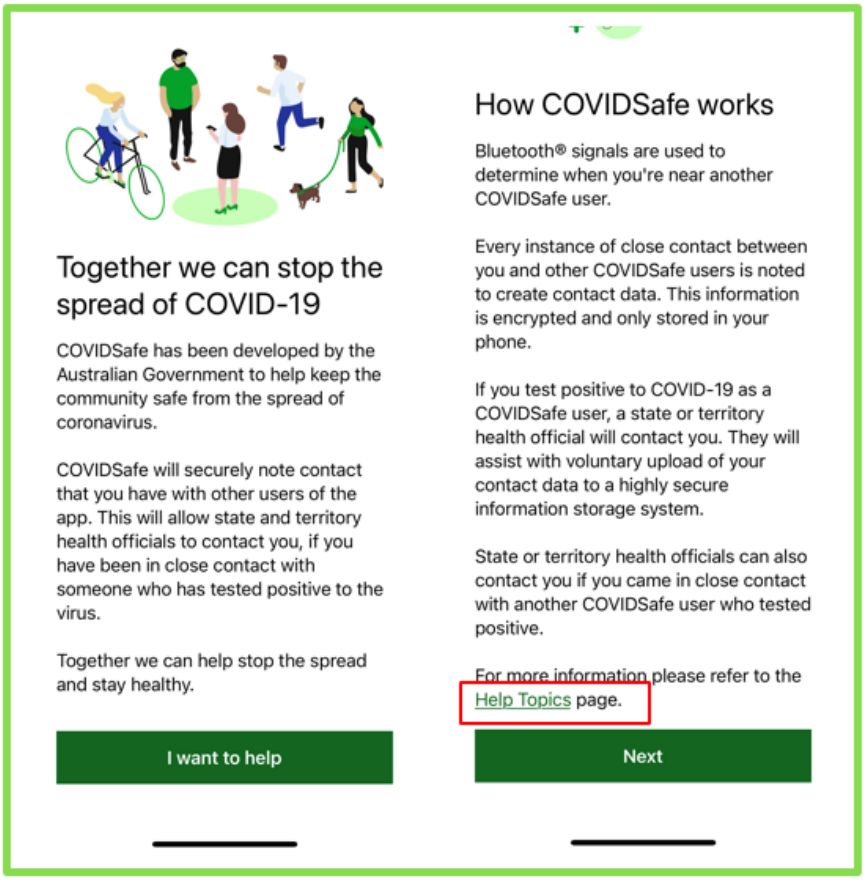


Figure 2: Background information of the COVIDSafe app and information, including help topics (highlighted by the red box), on how the COVIDSafe app works.

2.10 Once the user has read the 'How COVIDSafe works' section and selected 'Next', they are provided with a collection notice with the heading 'Registration and privacy'. The collection notice (see figure 3) details:

- that the use of the COVIDSafe app is voluntary
- that COVIDSafe users can install or delete the COVIDSafe app at any time

- the type of information that will be collected by the COVIDSafe app.

2.11 The collection notice contains 3 links (highlighted by the red boxes in figure 3) to the COVIDSafe Privacy Policy.

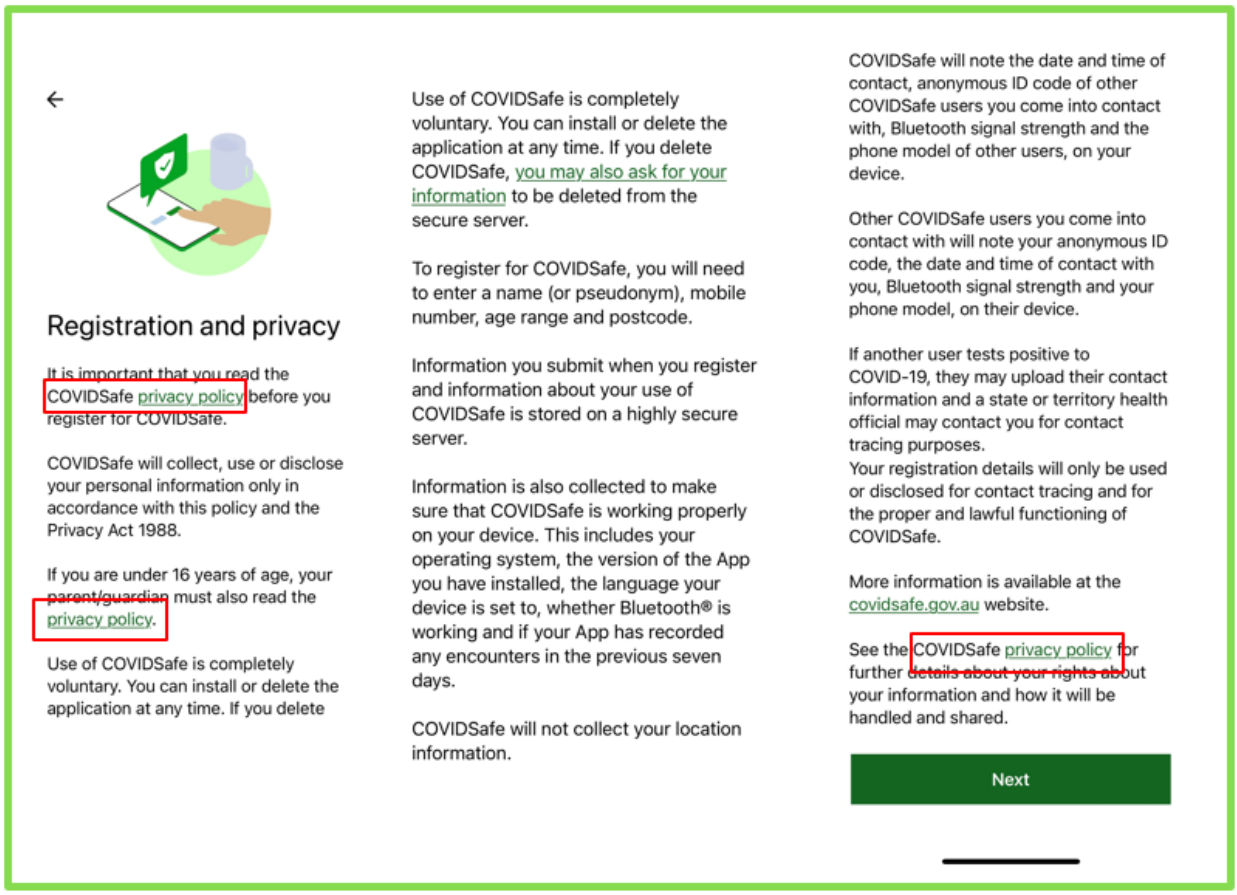


Figure 3: The collection notice provided to COVIDSafe users prior to registration. Including links to the COVIDSafe Privacy Policy (highlighted by the red boxes).

2.12 Once a COVIDSafe user has read the collection notice and selected 'Next', the app set up process directs them to another screen titled 'Registration consent' and they are asked to consent to the DTA collecting their personal information. Upon providing consent to the collection of their personal information as part of the registration process, the COVIDSafe user is prompted to enter their personal information as set out below (see figure 4).

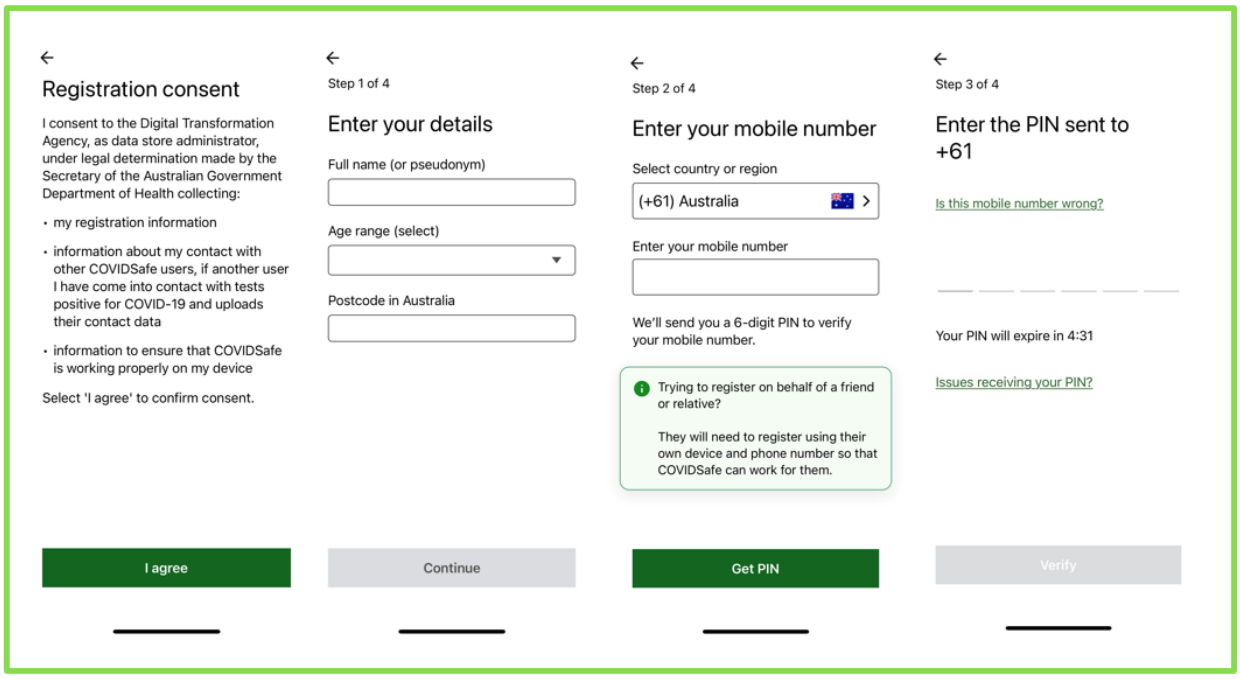


Figure 4: The consent provided to the DTA to collect personal information and registration process.

2.13 This consent is provided to allow the DTA, as the DSA, to collect:

- a user's registration information (including name (or pseudonym), age range, postcode and phone number) (Registration Data)
- information about the user's contact with other COVIDSafe users, in the event that another COVIDSafe user they have encountered tests positive to COVID-19 and uploads their contact data
- information to ensure that the COVIDSafe app is working properly on the user's device (Diagnostic Information), that being:
  - the operating system on the user's device
  - the version of the COVIDSafe app installed
  - the language the user's device is set to
  - whether Bluetooth is enabled on the user's device
  - whether the user has enabled battery optimisation on their device
  - whether the user's device has location services enabled, and
  - whether the COVIDSafe app has recorded any contact with other COVIDSafe users in the previous 7 days (being a 'yes' or 'no' response).

2.14 If the user is under 16 years old, they are prompted to have a parent/guardian provide consent to use the COVIDSafe app.

2.15 The final step of the registration process prompts the user to enable Bluetooth, notifications and location services, as required for the proper functioning of the COVIDSafe app (see figure 5).[3] Once the user has enabled these features the registration process is complete.

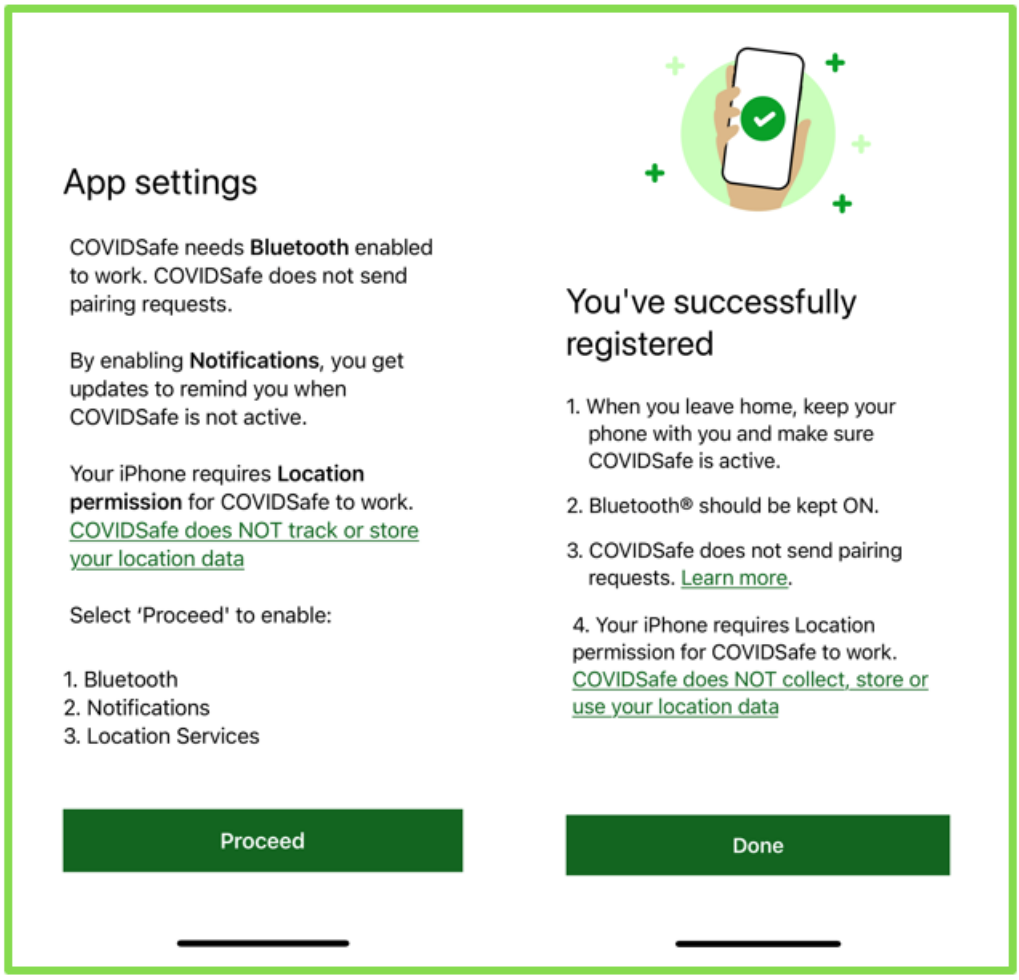


Figure 5: Confirming the COVIDSafe app settings required to ensure the proper functioning of the COVIDSafe app.

2.16 Once a COVIDSafe user is registered, an encrypted identifier (ID) is created for the COVIDSafe user, and their Registration Data is encrypted and stored in the NCDS.

[3] Android devices must have location services turned on for Bluetooth to operate. Activation of both Location Services and Bluetooth is a requirement on Android devices for any app, not just for the COVIDSafe app, that wishes to use Bluetooth to scan, connect or pair.

Use

2.17 The COVIDSafe app will exchange a user's information with other COVIDSafe users' devices when they come within 1.5 metres of each other (via a Bluetooth 'digital handshake'). The information exchanged is 'Contact Data' (as referred to in the COVIDSafe Privacy Policy) and consists of:

- user's encrypted ID
- date and time of the contact
- Bluetooth signal strength (which indicates the proximity of the contact)
- model of the device (phone) used.

2.18 A 'digital handshake' will be exchanged every 60 seconds that the COVIDSafe users' devices are within range. The information that is captured during a Bluetooth 'digital handshake' allows public health officials to determine if the COVIDSafe user is considered a 'close contact'. This is determined based on the number of digital handshakes where the COVIDSafe users were within 1.5 metres of each over a 15-minute period.

2.19 Contact Data that is exchanged via Bluetooth 'digital handshake' remains on a COVIDSafe user's device for a period of 21 days and is deleted from the device on a rolling basis.

Disclosure

2.20 When an individual receives a positive diagnosis for COVID-19, they may be asked by a STHA official if they have the COVIDSafe app and, if so, whether they consent (within the COVIDSafe app) to upload their Contact Data to the NCDS.

2.21 Where a COVIDSafe user consents to upload their Contact Data via the COVIDSafe app, the STHA official will log into the HOP to generate a PIN, and then the STHA official will provide the PIN to the COVIDSafe user, who will commence the upload process within the app (see figure 6). When a user consents to the upload they are also provided with a link to the COVIDSafe Privacy Policy (highlighted by the red box in figure 6 below).

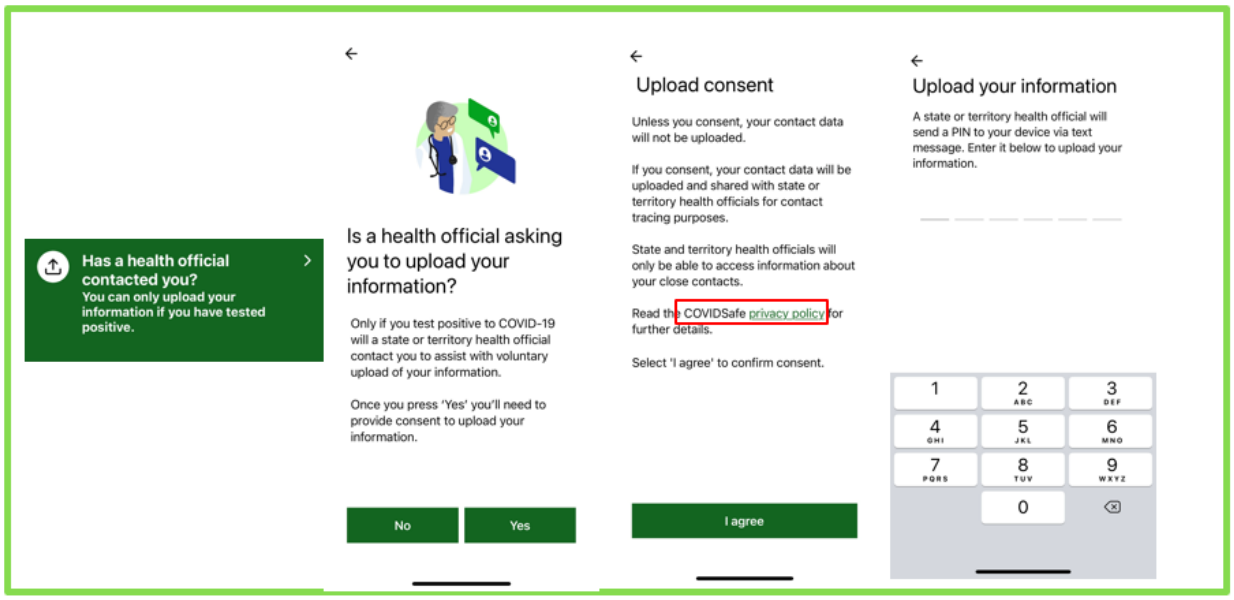


Figure 6: Consent to upload digital handshakes following a COVID-19 diagnosis.

2.22 Once a COVIDSafe user has selected 'I agree' and has entered the PIN, the COVIDSafe app will upload the past 21 days' worth of a COVIDSafe user's Contact Data to the NCDS. The Contact Data of the COVIDSafe user will be available to the relevant STHA officials via the HOP.

2.23 STHA officials can view the uploaded Contact Data by logging into the HOP. The HOP will display the status of the upload throughout this process and, once complete, will either identify that the upload was not successful, if the verification failed, no potential close contacts were found, or close contacts were identified.

2.24 A STHA official can filter the results to the time period in which the COVIDSafe user was infectious. If close contacts are identified, the results will be displayed, showing the STHA official a list of potential close contacts that the COVIDSafe user came into contact with. The STHA official can click on a potential close contact and filter the results based on probability that the contact was within 1.5 metres, the consistency of the contact and whether it meets the predefined algorithm threshold (this algorithm is based on the number of digital handshakes over a 15 minute period).

2.25 The STHA official will identify any close contacts (who are COVIDSafe users) that may not have already been identified through the STHA's other contact tracing processes and the STHA official will be able to contact these close contacts. At this point, the STHA official will verify or recollect personal information of the COVIDSafe user, which has the effect of changing the status of this information from COVID app data to a state or territory health record.[4]

[4] COVIDSafe Assessment 2 assesses access controls applied to COVID app data by State and Territory health authorities and at the time of the publication of this report was not finalised.

Deletion

2.26 COVID app data that is collected during the operation of the COVIDSafe app is stored on a COVIDSafe users' device for a period of 21 days. After this period the COVID app data is deleted from the COVIDSafe user's device and is no longer accessible.

2.27 Registration Data stored in the NCDS is not automatically deleted after 21 days but can be deleted at the request of a COVIDSafe user via a webform ('Request data deletion' Webform) available on the COVIDSafe website. However, COVID app data, including Registration Data must be deleted from the NCDS as soon as practicable after the end of the COVIDSafe data period.[5] COVIDSafe Assessment 4 considers the retention, destruction and deletion of COVID app data.[6]

Changes to the COVIDSafe app and COVIDSafe System

2.28 Since the COVIDSafe app was first launched on 26 April 2020, there have been multiple changes to the environment in which the app operates, including changes to the law, and a number of internal design and implementation factors, such as technical developments, that have required changes and updates be made to the COVIDSafe app and the wider COVIDSafe System.

2.29 In conducting this assessment, the OAIC considered the external and internal events that resulted in updates and amendments being made to the COVIDSafe app and COVIDSafe System from April to December 2020. These changes have the potential to change the way in which COVID app data is handled by entities.

2.30 For example, changes to the functionality of the COVIDSafe app could alter the way in which COVID app data is collected by the DSA; such changes may require amendments to be made to the COVIDSafe Privacy Policy and collection notices to ensure those documents accurately reflect the new information handling practices.

2.31 While changes to the COVIDSafe System (in particular, the NCDS and HOP) are examined in the COVIDSafe Assessment 1 report, the OAIC considers those changes are also relevant to the scope of this privacy assessment given that changes to the ways in which COVID app data is handled (collected, used, held, disclosed and secured) may require amendments to be made to the COVIDSafe Privacy Policy and collection notices.

2.32 At Appendix E the OAIC has graphically represented the major external and internal factors that resulted in changes to the COVIDSafe app, COVIDSafe System, COVIDSafe Privacy Policy and collection notices. A short overview of each of those factors is set out in the following paragraphs.

---

[5] The end of the COVIDSafe data period is determined under s 94Y of the Privacy Act.

[6] At the time of publication of this assessment report, COVIDSafe Assessment 4 was not finalised.

External factors impacting COVIDSafe

2.33 The OAIC observed that external factors influencing the operating context of the COVIDSafe app included (but were not limited to) legislative, government policy and administrative developments in response to the pandemic, including developments relating to privacy, public health and contact tracing.

2.34 Generally, changes to privacy legislation accounted for the greatest external impact on the COVIDSafe System and changes to the design and implementation of the COVIDSafe app. Major legislative changes impacting the COVIDSafe System, and COVIDSafe app include:

- the Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements—Public Health Contact Information) Determination 2020 (Cth) (the Biosecurity Determination), which was made by the Minister for Health on 25 April 2020 under subsection 477(1) of the *Biosecurity Act 2015* (Cth), immediately prior to the launch of the COVIDSafe App
- the *Privacy Amendment (Public Health Contact Information) Act 2020* (Privacy Amendment Act), which was passed by the Australian Parliament on 14 May 2020 and introduced Part VIIIA to the Privacy Act to protect COVID app data and provide the OAIC with an oversight and assurance role over the COVIDSafe System
- the Privacy Amendment (Public Health Contact Information) (Data Store Administrator) Determination 2020, which was made by the Secretary of the Department of Health on 15 May 2020 under subsection 94Z(1) of the Privacy Act, appointing the DTA as DSA for the NCDS.

2.35 Appendix E sets out these legislative changes alongside updates to the COVIDSafe app and the Privacy Policy and Collection Notice, while Appendix A provides further detail on the legislation governing the COVIDSafe System.

2.36 The OAIC also observed that changes in administrative arrangements between the DoH, DTA and STHA, and changes to government policy impacted the development of the COVIDSafe System. These changes include:

- the Memorandum of Understanding between the DoH and DTA executed 5 August 2020.
- the Bilateral Agreements between the Commonwealth and each STHA on the collection, use and disclosure of COVID app data executed for:
  - Australian Capital Territory on 11 May 2020
  - New South Wales on 8 May 2020
  - Northern Territory on 8 May 2020
  - Queensland on 8 May 2020

  - South Australia on 8 May 2020
  - Tasmania on 8 May 2020
  - Victoria on 8 May 2020
  - Western Australia on 8 May 2020
- various policy decisions made by the Australian Government relating to the operation of the COVIDSafe system, including the decision to not enable STHA to download COVID app data through the HOP.

2.37 Most administrative and policy changes to the COVIDSafe System were found to relate to the operation and maintenance of the NCDS and HOP, and not the COVIDSafe app itself; these matters are examined in greater detail as part of COVIDSafe Assessment 1 and COVIDSafe Assessment 2 which focus on the NCDS and HOP.[7] However, some reference is made to these administrative and policy changes to the COVIDSafe System in this report to the extent that those matters resulted in amendments to the COVIDSafe Privacy Policy.

Internal factors

2.38 The OAIC also found numerous factors internal to the DSA and app development team which resulted in changes to the COVIDSafe app's design and implementation. These were mostly technical in nature, and included (but were not limited to):

- bug fixes
- security and privacy updates
- changes to app functionality
- useability enhancements, such as:
  - additional languages
  - additional COVID-19 related content
- accessibility enhancements.

2.39 At the time fieldwork concluded on 24 December 2020, 17 updates had been made concurrently to the COVIDSafe app for iOS Systems and Android based systems. These updates included those in relation to the implementation of the Herald Bluetooth protocol which was released on 19 December 2020, and which changed the way in which devices use Bluetooth to identify other devices within the appropriate range (1.5 metres).

[7] At the time of publication of this assessment report, COVIDSafe Assessment 2 State and Territory Health Authorities Access Controls was not finalised.

COVIDSafe legislative framework

2.40 The personal information collected by the COVIDSafe app through the COVIDSafe System has been protected by the following:

- the Biosecurity Determination (from 25 April until 15 May 2020)
- the Privacy Act, which includes:
  - the APPs
  - Part VIIIA – Public health contact information (from 16 May 2020 onwards).

2.41 The COVIDSafe legislative framework has been described in detail in the COVIDSafe Assessment 1 report. This information has also been included in Appendix A for reference.

Role of the OAIC

2.42 The new Part VIIIA of the Privacy Act has granted the Australian Information Commissioner (AIC) a range of additional proactive and reactive regulatory powers which support the AIC's legislated functions in relation to the handling of personal information in the COVIDSafe System.

2.43 The OAIC engaged PricewaterhouseCoopers (PwC) under s 24 of the *Australian Information Commissioner Act 2010* (Cth) to assist the OAIC with the COVIDSafe Assessment Program. PwC worked jointly with OAIC staff to assist the AIC to conduct elements of the fieldwork for this assessment.

2.44 While assessing the general compliance of the COVIDSafe Privacy Policy with APPs 1.3 and 1.4, the OAIC's assessment determined there was a potential issue with the extent to which the COVIDSafe Privacy Policy was prominently displayed, accessible and easy to download for users. As this issue was outside the initial scope of this assessment, the OAIC decided to expand the scope of the assessment to also consider compliance with APP 1.5.

2.45 The role of the OAIC has been described in detail in COVIDSafe Assessment 1. This information has also been included in Appendix B for reference.

Part 3: Findings

Our approach

3.1 The key findings of the Assessment are set out below under the following headings and sub-headings:

- APP 1 – open and transparent management of personal information
  - APP 1.3 – Requirement to have APP Privacy Policy
  - APP 1.4 – Information that must be included in an APP Privacy Policy
  - APP 1.5 – Making an APP Privacy Policy publicly available.
- APP 5 – notification of the collection of personal information
  - APP 5.1 – Collection notices
  - APP 5.2 – APP 5 matters.
- Part VIIIA of the Privacy Act
  - section 94D – Collection, use or disclosure of COVID app data
  - section 94E – COVID app data on communication devices
  - section 94F – COVID app data in the National COVIDSafe Data Store
  - section 94G – Decrypting COVID app data.

3.2 For each key finding, we have outlined the relevant control frameworks or measures, a summary of observations, the privacy risks arising from the observations, followed by opportunities to address identified privacy risks.

3.3 As part of this Assessment, the OAIC considered the following control frameworks (see Appendix C for full details):

- Attorney-General's Department (AGD) Protective Security Policy Framework (PSPF) core requirements:
  - Policy 8
  - Policy 9
  - Policy 10
  - Policy 11.
- Australian Government Information Security Manual (ISM) principles:

- G2, G3, G4, G5
- P1, P2, P3, P4, P5, P6, P7, P8, P10, P11, P12, P13, P14
- D1.

- International Organization for Standardization (ISO)/International Electrotechnical Commissioner (IEC) 27001 sections:
  - 5.2
  - 6.1, 6.2
  - 7.2, 7.5
  - 8.1, 8.2, 8.3
  - 9.1
  - 10.1, 10.2.
- ASAE3150 Assurance Engagement on Controls.

3.4 As part of this Assessment, the OAIC also considered the following control measures (see Appendix A for full details), which relate to the NCDS and the handling of COVID app data:

- APP Guidelines, which outline the mandatory requirements of the APPs, best practice recommendations for achieving compliance with the APPs, the way in which the OAIC will interpret the APPs and matters the OAIC may take into account when exercising functions and powers under the Privacy Act
- COVIDSafe app PIA.

3.5 Given the scale and sensitivity of COVID app data collection by the Australian Government, the OAIC considers it reasonable that a robust and comprehensive approach to the protection of personal information would be in place for the COVIDSafe System.

APP 1 – open and transparent management of personal information

3.6 The objective of APP 1 is to ensure APP entities manage personal information in an open and transparent way. This enhances the accountability of APP entities for their personal information handling practices and can build community trust and confidence in those practices.

3.7 The specific obligations APP 1 imposes on an APP entity, that are within the scope of this assessment, are to:

- have a clearly expressed and up-to-date privacy policy about how the entity manages personal information (APPs 1.3 and 1.4)
- take reasonable steps to make its APP privacy policy available free of charge in an appropriate form (APP 1.5).

3.8 This section examines the design and technical implementation of the COVIDSafe app, and the COVIDSafe Privacy Policy against the requirements of APP 1.3, 1.4 and 1.5, specifically:

- APP 1.3 – Requirement to have an APP Privacy Policy that is
  - accurate (clearly expressed)
  - current (up to date).
- APP 1.4 – Information that must be included in an APP Privacy Policy
  - kinds of personal information collected and held (APP 1.4(a))
  - how personal information is collected and held (APP 1.4(b))
  - purpose for which the entity collects, holds, uses and discloses personal information (APP 1.4(c))
  - access and correction of personal information (APP 1.4(d))
  - privacy complaints (APP 1.4(e))
  - overseas Disclosures (APP 1.4(f) and (g))
- APP 1.5 – Making an APP Privacy Policy publicly available.

3.9 For the purpose of this Assessment, the OAIC had regard to Chapter 1 of the APP Guidelines, which provide guidance to APP entities on clear expression of information handling practices and requirements for currency of APP Privacy Policies.

APP 1.3 - Requirement to have an APP Privacy Policy

3.10 APP 1.3 outlines the requirement for APP entities to have a clearly expressed and up to date privacy policy about how the APP entity manages personal information.

3.11 An APP Privacy Policy should explain how the APP entity manages personal information, and the information flows associated with that personal information. The requirement to have an APP Privacy Policy reflects the central object of APP 1, which is to ensure that entities manage personal information in an open and transparent manner.

3.12 The APP Privacy Policy must be tailored to the specific information handling practices of an entity. In some cases, such as with the COVIDSafe app, a subset of an entity's information handling practices may necessitate a separate standalone policy, particularly where those

practices relate to the handling of sensitive information or complex processes requiring further explanation.

3.13 While an APP Privacy Policy is not expected to contain detail about all the practices, procedures and systems adopted to ensure APP compliance, it must be clearly expressed, and up to date. An APP Privacy Policy should also be directed to the different audiences who may consult it: primarily this will be individuals whose personal information is, or is likely to be, collected or held by the APP entity.

3.14 As the DSA, the DTA is the APP entity responsible for maintaining and updating the COVIDSafe Privacy Policy. The OAIC understands that the DTA has, when developing, maintaining and updating the COVIDSafe Privacy Policy, sought input and advice from the DoH as the policy owner of the COVIDSafe System and the department responsible for the Australian Government's COVID-19 response.

3.15 To gauge the compliance of the Australian Government, as represented by DoH and DTA, against the requirements of APP 1.3, the OAIC examined:

- the accuracy of the COVIDSafe Privacy Policy
- the currency of the COVIDSafe Privacy Policy.

3.16 To assess the accuracy and currency of the COVIDSafe Privacy Policy, the OAIC examined the functionality of the COVIDSafe app and broader COVIDSafe System by:

- conducting a document review of the COVIDSafe Privacy Policy, design and technical documents and Jira[8] tickets related to key changes within the COVIDSafe app
- interviewing key DoH and DTA staff responsible for the design and implementation of the COVIDSafe System
- conducting a review of the source code of the COVIDSafe app.

Accuracy of APP Privacy Policy

3.17 To comply with APP 1.3, an APP entity must have a clearly expressed privacy policy that details how the APP entity manages personal information. At a minimum, a clearly expressed privacy policy should be easy to understand (avoiding jargon, legalistic and in-house terms), easy to navigate, and only include information that is relevant to the management of personal information by the entity.

3.18 In conducting this assessment, the OAIC reviewed the current version of the COVIDSafe Privacy Policy and COVIDSafe System, as well as the changes to both the policy and the COVIDSafe System since it was first implemented.

[8] Jira is a proprietary issue tracking product developed by Atlassian that allows bug tracking and agile project management.

3.19 The OAIC also reviewed the Privacy Assurance Assessment developed in relation to the introduction of the functionality to collect Diagnostic Information and the updated COVIDSafe Privacy Policy issued on 25 September 2020. Following this review the OAIC is satisfied that the changes to the COVIDSafe Privacy Policy as a result of this change accurately reflect the collection, use and disclosure of the Diagnostic Information.

3.20 The OAIC found that both the current and former versions of the COVIDSafe Privacy Policy accurately and clearly describe the process for the collection, use and disclosure of personal information by the DTA, as the DSA, in relation to the COVIDSafe app, including:

- how personal information (e.g. Registration Data, Contact Data and Diagnostic Information) is collected
- how that personal information is used and disclosed
- how personal information is stored (both via the NCDS and on the user's communication device)
- whether personal information can be deleted
- whether a user can correct or access their personal information.

3.21 The OAIC has also verified that the source code of the COVIDSafe app was consistent with statements made by the DoH and DTA personnel interviewed in relation to the design and implementation of the COVIDSafe app. Information was verified by reviewing the source code of the COVIDSafe app, published publicly on GitHub by the DTA. This review confirmed that the source code aligned to the design and technical documentation provided by the DTA, as well as the personal information handling procedures detailed in the COVIDSafe Privacy Policy.

3.22 In addition, the OAIC reviewed the current version of the COVIDSafe Privacy Policy against the OAIC's understanding of the COVIDSafe System functionality and found that the COVIDSafe Privacy Policy accurately describes the functionality of the COVIDSafe System in relation to the management of personal information. While this assessment is a point in time assessment, the OAIC also considered the accuracy of previous versions of the COVIDSafe Privacy Policy and found that these versions accurately reflect the functionality of the COVIDSafe System at the time these policies were in place.

3.23 The OAIC has also reviewed the PIA developed in relation to the use of the Herald Bluetooth protocol and the updated COVIDSafe Privacy Policy issued on 16 December 2020. Following this review, the OAIC is satisfied that the amendments to the Privacy Policy as a result of the introduction of the Herald Bluetooth protocol accurately reflect the new method for collecting personal information.

3.24 The OAIC considers that the COVIDSafe Privacy Policy is, overall, clearly expressed in appropriate language for the intended audience and avoids the use of jargon, legalistic and in-house terms. The COVIDSafe Privacy Policy has been developed using a layered approach, with

each section laid out in a logical sequence to assist users to understand the management of their personal information and when and how it will be collected, used and disclosed. The OAIC notes the current and superseded versions of the COVIDSafe Privacy Policies refer to the 'encrypted user ID' that is created every 7 days for users of the COVIDSafe app, however current and superseded versions of the COVIDSafe Privacy Policies do not provide users with any explanation of what the 'encrypted user ID' is. This results in a low privacy risk as the policy does not contain a clear explanation of what this term means. The OAIC suggests that the DTA includes a brief description of how the encrypted user ID is created and assigned to each user so that the COVIDSafe Privacy Policy is more clearly expressed and easier to understand.

Suggestion 1
The OAIC suggests the DTA update the COVIDSafe Privacy Policy with a brief explanation of how the encrypted user ID is created and assigned to each user.

3.25 The OAIC further notes that, while the COVIDSafe Privacy Policy is, overall, clearly expressed in appropriate language, given it is likely to be predominately accessed by users on a mobile device, the clarity and readability of the COVIDSafe Privacy Policy would be enhanced by implementing measures outlined in the OAIC's *Mobile privacy: a better practice guide for mobile app developers* guidance, such as making use of graphics to communicate concepts, as well using colour to emphasise key aspects of the privacy policy.

Currency of APP Privacy Policy

3.26 APP 1.3 also requires APP entities to have an up-to-date privacy policy about the management of personal information by the entity.

3.27 As noted in paragraphs 2.28 - 2.37, the OAIC found that updates to the COVIDSafe Privacy Policy are generally a result of either legislative change, policy changes, or administrative or technical changes to the COVIDSafe app. However not all technical or policy driven changes, require a change to the policy.

3.28 The initial version of the COVIDSafe Privacy Policy was developed based on the Biosecurity Determination (see Appendix A for further detail). This version of the policy was published and had effect from 26 April 2020.

3.29 The COVIDSafe Privacy Policy was subsequently updated following the introduction of the Privacy Amendment Act (see Appendix A) to account for legislative changes to the framework governing the COVIDSafe System and the subsequent appointment of the DTA as the DSA on 14 and 15 May 2020 respectively. The Privacy Amendment Act introduced a substantial overhaul of the legislative regime governing the COVIDSafe system and expanded the legislative basis on which the COVID app data could be collected, used and disclosed.

3.30 The COVIDSafe Privacy Policy was updated to reflect these developments on 7 July 2020. This update revised the description of how the DTA handles COVID app data in accordance with the revised legislative regime, however this update was made 53 days after those changes came into effect.

3.31 During fieldwork interviews, the DTA advised that they are developing the COVIDSafe System via an agile delivery methodology.[9] The DTA captures technical changes through Jira, added to the product backlog[10] and changes are assessed as part of the COVIDSafe app roadmap and prioritised during sprint planning.

3.32 The DTA advised that a 'privacy by design' approach is taken to development of the COVIDSafe System and privacy is considered as part of all stages of development. This is evidenced by the different privacy assessments that are undertaken by the DTA during the development of functionality within the COVIDSafe system, including:

- **an informal privacy threshold assessment**: an initial assessment as to whether the proposed change or enhancement will have an impact on the privacy of a COVIDSafe user
- **a Privacy Assurance Assessment**: an internal privacy assessment undertaken by the DTA to determine what impact the proposed change or enhancement will have on the privacy of COVIDSafe users
- **a Privacy Impact Assessment (PIA)**: a systematic assessment of a change or enhancement that identifies the impact that the change or enhancement might have on the privacy of COVIDSafe users.

3.33 The DTA advised that all proposed changes to the COVIDSafe System have an informal privacy threshold assessment conducted by the DTA's COVIDSafe app project team. Through this process the project team will consider the privacy impact of the change and determine what level of assessment may be needed in relation to the change, this has been documented in Jira tickets. While the DTA advised this is undertaken for all changes, not all Jira tickets were provided for to the OAIC to review, so the OAIC was unable to confirm if this assessment was undertaken for all changes.

3.34 Based on this initial threshold assessment there may be no privacy implication identified, or if there are privacy implications, the DTA advised that it would undertake an internal Privacy Assurance Assessment or commission a full PIA. These assessments also determine whether any changes are required to the COVIDSafe Privacy Policy.

[9] An Agile delivery methodology is a project management approach based on delivering requirements iteratively and incrementally throughout the software development life cycle.

[10] A product backlog is a list of the new features, changes to existing features, bug fixes, infrastructure changes or other activities that a team may deliver in order to achieve a specific outcome.

3.35 The OAIC considers that the time period between the introduction of the Privacy Amendment Act and the update of the COVIDSafe Privacy Policy would have given rise to a low privacy risk that users did not understand how the DTA would manage their personal information. This is because the DTA did not maintain an up-to-date privacy policy as required by APP 1.3. However, as this version of the COVIDSafe Privacy Policy has now been superseded, the OAIC has not made a suggestion in relation to this matter.

3.36 The COVIDSafe Privacy Policy was also updated in relation to the introduction of additional functionality to the COVIDSafe app to facilitate the collection of Diagnostic Information from COVIDSafe users' devices to ensure the proper function of the COVIDSafe app. The DTA undertook a Privacy Assurance Assessment of the additional functionality to identify the potential impact on the collection, use and disclosure of personal information. This assessment identified that additional personal information would potentially be collected as part of Diagnostic Information and, as a result, the COVIDSafe Privacy Policy was updated to reflect this. This additional functionality, and the updated COVIDSafe Privacy Policy was introduced on 25 September 2020.

3.37 The introduction of the Herald Bluetooth protocol also resulted in an update to the COVIDSafe Privacy Policy, based on a PIA conducted by Australian Government Solicitors (AGS) in November 2020. While the PIA did not identify any additional personal information being collected, the change did introduce new ways in which COVID app data may be collected. Therefore, the privacy policy was updated to reflect this change. The introduction of the Herald Bluetooth protocol occurred on 19 December 2020 and the updated COVIDSafe Privacy Policy took effect on 16 December 2020.

3.38 While the update to the COVIDSafe Privacy Policy took 53 days to be published following the Privacy Act Amendment being introduced, a timeframe the OAIC does not consider reasonable, subsequent updates (based on functionality change to the COVIDSafe app) to the COVIDSafe Privacy Policy have been issued concurrently with the introduction of changes to the functionality of the COVIDSafe app. This demonstrates significant improvement by the DTA in updating the COVIDSafe Privacy Policy to ensure it is accurate and up to date. This suggests to the OAIC that adequate procedures and systems are in place to ensure the timely update of the COVIDSafe Privacy Policy following a major policy or technical change to the COVIDSafe app.

3.39 Therefore, the OAIC does not consider there to be any systemic issue relating to updating the COVIDSafe Privacy Policy in accordance with the requirements of APP 1.3, and is satisfied with the process that the DTA undertakes to update the COVIDSafe Privacy Policy.

3.40 The OAIC considers that, as a result of its review of the current and legacy version of the COVIDSafe Privacy Policy, the design and technical implementation of the COVIDSafe System (including the source code of the COVIDSafe app), the DTA has had an up-to-date privacy policy for the COVIDSafe app. In addition, this policy has been updated within a reasonable time to reflect changes to the legislative regime governing, and technical changes to the function of,

the COVIDSafe app, with the exception of the initial update to the COVIDSafe Privacy Policy introduced on 7 July 2020, which was not updated in a reasonable time.

Key finding: The OAIC is **satisfied** that the Data Store Administrator has provided a clearly expressed and up to date policy about the management of COVID app data in accordance with APP 1.3.

APP 1.4 - Information that must be included in an APP Privacy Policy

3.41 APP 1.4 requires APP entities to include certain information in their APP Privacy Policy so that readers can understand how their personal information will be handled by the entity, how they may access and correct their information, and how they may make a privacy complaint to the entity.

3.42 At a minimum, APP 1.4 requires that an APP Privacy Policy include:

- the kinds of personal information that entity collects and holds (APP 1.4 (a))
- how the entity collects and holds personal information (APP 1.4 (b))
- the purposes for which the entity collects, holds, uses and discloses personal information (APP 1.4 (c))
- how an individual may access personal information held by the entity and seek the correction this information (APP 1.4 (d))
- how an individual may complain about a breach of the of the APPs, or a registered APP code that binds the entity, and how the entity will deal with such a complaint (APP 1.4(e))
- whether the entity is likely to disclose personal information to overseas recipients (APP 1.4 (f)), and if so, the countries in which the recipients are likely to be located (APP 1.4 (g)).

Kinds of personal information that entity collects and holds (APP 1.4 (a))

3.43 An APP Privacy Policy must describe, in general terms, the kinds of personal information an APP entity usually collects and holds.

3.44 The OAIC reviewed the COVIDSafe Privacy Policy, the design documentation, the technical documentation and source code of the COVIDSafe app to determine whether the detail provided in the policy accurately describes the kind of personal information that is collected and held as a result of a user using the Australian Government's COVIDSafe app.

3.45 As noted above, the personal information collected in connection with the use of the COVIDSafe app is the Registration Data (outlined in paragraph 2.13) the Contact Data (outlined in paragraph 2.17) and the Diagnostic Information (outlined in paragraph 2.13).

3.46 The OAIC reviewed the COVIDSafe Privacy Policy issued on 16 December 2020, and all superseded versions of the COVIDSafe Privacy Policy, and confirmed that these versions of the policy accurately describe the type of personal information that is collected and held in connection with the COVIDSafe app.

How the entity collects and holds personal information (APP 1.4 (b))

3.47 APP 1.4(b) requires that an APP Privacy Policy explain an APP entity's usual approach to collecting and holding personal information. This should include how the entity stores and secures personal information.

3.48 The OAIC reviewed the COVIDSafe Privacy Policy, the design documentation, the technical documentation and source code of the COVIDSafe app to determine whether the detail provided in the COVIDSafe Privacy Policy aligns to the design and technical implementation of the COVIDSafe System, as it relates to the way personal information is collected and held.

3.49 The COVIDSafe app is the only method for collecting or creating personal information that is considered COVID app data. This personal information is:

- Registration Data, via the process detailed in paragraphs 2.12, 2.13 and figure 4
- Contact Data, via the process outlined in paragraph 2.17 and 2.18, when COVIDSafe users are within range (1.5 metres) of each other and the COVIDSafe app is active
- Diagnostic Information, outlined in paragraph 2.13, collected via the day-to-day use of the COVIDSafe app.

3.50 Following the review referred to in para 3.48 above, the OAIC found that this process is consistent with the description of the process provided in the current and superseded versions of the COVIDSafe Privacy Policy.

3.51 Under APP 1.4(b), an APP Privacy Policy must also describe an APP entity's usual approach to holding personal information. This should include how the entity stores and secures personal information.

3.52 COVID app data is stored in the NCDS, and this is accurately described in the COVIDSafe Privacy Policy. In assessing the COVIDSafe Privacy Policy against APP 1.4, the OAIC reviewed the processes for storing and maintaining COVID app data in the NCDS. The assessment confirmed that the COVIDSafe Privacy Policy complies with the requirements of APP 1.4(b) by accurately describing how COVID app data is held within the NCDS, and how and the duration it is held, on a COVIDSafe user's communication device.

Purpose for which the entity collects, holds, uses and discloses personal information (APP 1.4 (c))

3.53 An APP Privacy Policy must describe the purposes for which personal information is usually collected, held, used and disclosed (APP 1.4(c)).

3.54 The OAIC reviewed the COVIDSafe Privacy Policy, the design documentation, the technical documentation and source code of the COVIDSafe app to determine whether the detail provided in the COVIDSafe Privacy Policy aligns to the design and technical implementation of the COVIDSafe System, as it relates to the way personal information is collected, held, used and disclosed.

3.55 The OAIC's review confirmed that the COVIDSafe Privacy Policy complies with APP 1.4 (c) by accurately describing the purposes for which COVID app data is collected, held used and disclosed, being:

- to enable contact tracing by STHA. To enable this process, the DTA has developed the HOP, as detailed in paragraphs 2.21-2.25
- in respect of the Diagnostic Information, to ensure the proper operation of the COVIDSafe app
- to produce de-identified statistical information about the total number of registrations through COVIDSafe app
- to confirm that the correct data is being deleted, when an individual makes a request to delete their personal information held in the NCDS
- to permit the AIC to perform functions or exercise powers under or in relation to Part VIIIA of the Privacy Act
- if necessary, for the purposes of investigation and prosecution of a breach under Part VIIIA of the Privacy Act.

How an individual may access personal information held by the entity and correct this information (APP 1.4 (d))

3.56 An APP Privacy Policy must explain the procedure an individual can follow to gain access to or seek correction of personal information the APP entity holds (APP 1.4(d))

3.57 While APP 1.4(d) outlines the requirement for an APP entity to advise how an individual may exercise their right under APP 12.1 to access their personal information held by an APP entity, COVID app data is governed by Part VIIIA of the Privacy Act.

3.58 Section 94D(2) of the Privacy Act makes it an offence to collect, use or disclose data that is COVID app data except in specified circumstances including:

- by authorised STHA officials for contact tracing purposes (s 94D(2)(a))
- by DTA staff or contracted service providers for contact tracing purposes or to ensure the proper functioning, integrity and security of the COVIDSafe System (s 94D(2)(b))
- where the collection or use is for the purposes of transferring encrypted data between communication devices through the COVIDSafe app or between the COVIDSafe app and the NCDS (s 94D(2)(c)).

3.59 Providing a COVIDSafe user with access to their COVID app data is not an exception to s 94D(2). Section 94ZD(1) of the Privacy Act prevents individuals from being able to access their personal information that is considered COVID app data. This is because of the operation of this section cancels the effect of a provision of any Australian law (other than Part VIIIA of the Privacy Act) that would have the effect of permitting or requiring conduct, or an omission to act, that would otherwise be prohibited under Part VIIIA of the Privacy Act.

3.60 While the COVIDSafe Privacy Policy advises that COVIDSafe users will not be able to access their COVID app data to 'ensure maximum security of your COVIDSafe data', the policy does not outline that this is not permitted due to the operation of ss 94D(2) and 94ZD(1) of the Privacy Act.

3.61 This results in the low privacy risk that COVIDSafe users may not appreciate that their APP 12 access rights do not apply to COVID app data, and they may attempt to seek access to their COVID app data. To better address compliance and limit this misconception, the OAIC suggests that the DTA amends the COVIDSafe Privacy Policy to clarify for COVIDSafe users that access to their COVID app data is not permitted by law.

Suggestion 2
The OAIC suggests that the DTA update the COVIDSafe Privacy Policy to advise COVIDSafe users that access to their COVID app data is not permitted by law.

3.62 APP 1.4(d) also outlines the requirement for an APP entity to advise how an individual can correct their personal information. The DTA has implemented a process to enable the correction of user-entered personal information, whereby a COVIDSafe user can request the deletion of their Registration Data and then re-register with the correct information. The OAIC confirmed that the COVIDSafe Privacy Policy has described this process accurately.

How an individual may complain about a breach of the of the APPs, or a registered APP code that binds the entity, and how the entity will deal with such a complaint (APP 1.4(e))

3.63 An APP Privacy Policy must explain how an individual can complain about an APP entity's breach of the APPs or a binding registered APP code (APP 1.4(e)).

3.64 The COVIDSafe Privacy Policy sets out the process by which an individual can make a complaint to the DTA, the OAIC or the Australian Federal Police, and this complies with the requirement of APP 1.4(e).

Whether the entity is likely to disclose personal information to overseas recipients (APP 1.4 (f)), and if so, the countries in which the recipients are likely to be located (APP 1.4 (g)).

3.65 An APP Privacy Policy must set out whether personal information is likely to be disclosed to overseas recipients and the countries in which such recipients are likely to be located 'if it is practicable to specify those countries in the policy' (APP 1.4(f) and 1.4(g)).

3.66 APP 1.4(f) and (g) require that an APP entity's privacy policy identify if the disclosure of personal information will likely occur to an overseas recipient. Pursuant to s 94F of the Privacy Act, it is an offence in certain circumstances for COVIDSafe data to be held on a database outside Australia and for a person to disclose COVIDSafe data to a person overseas. The NCDS is hosted by AWS and the DTA has determined that COVID app data in the NCDS will only be stored in Australia. Further information relating to the compliance of the DTA, as the DSA, in relation to compliance with s 94F is provided in COVIDSafe Assessment 1.

Key finding: The OAIC is **satisfied** that the COVIDSafe Privacy Policy, and the implementation of the COVIDSafe System meets the requirements of APP 1.4.

APP 1.5 – Availability of APP privacy policy

3.67 APP 1.5 requires an APP entity to take reasonable steps to make its APP privacy policy available free of charge, and in an appropriate form.

3.68 An APP entity is generally expected to make its policy available by publishing it on its website. The policy should be prominently displayed, accessible and easy to download. Where it is foreseeable that the policy may be accessed by individuals with special needs (such as individuals with a vision impairment, or individuals from a non-English speaking background), appropriate accessibility measures should be put in place. Government agencies are also required to comply with any applicable government accessibility requirements, such as achieving a Web Content Accessibility Guidelines (WCAG)[11] 2.0 Level AA rating.

3.69 While assessing the general compliance of the COVIDSafe Privacy Policy with APP 1.3 and 1.4, the OAIC's assessment determined there was a potential issue with the extent to which the COVIDSafe Privacy Policy was prominently displayed, accessible and easy to download for

[11] The WCAG documents explain how to make web content more accessible to people with disabilities https://www.w3.org/WAI/standards-guidelines/wcag/

users. As this issue was outside the initial scope of this assessment, the OAIC elected to expand the scope of the assessment to consider compliance with APP 1.5.

3.70 The OAIC notes that the COVIDSafe app (including the COVIDSafe Privacy Policy) was assessed by Vision Australia in July 2020 for conformance against the WCAG Level 2.1 Guidelines and achieved a Level AA ranking. As conformance with Level 2.1 would also demonstrate compliance with WCAG 2.0, the OAIC is satisfied that the DTA has complied with applicable accessibility requirements.

3.71 The OAIC's assessment of whether the COVIDSafe Privacy Policy is prominently displayed, accessible and easy to download found that:

- during the registration process, users are provided with 3 links to the COVIDSafe Privacy Policy (see paragraph 2.11)
- once registered, a COVIDSafe user can only access the COVIDSafe Privacy Policy via the 'help topics' section of the front page of the COVIDSafe app. Once a user has accessed the 'help topics' section, they must scroll to the very bottom of the page to access the COVIDSafe Privacy Policy via a hyperlink in the navigation pane.
- alternatively, users may access the privacy policy by scrolling to the 'More Information on COVIDSafe' section to access the COVIDSafe Privacy Policy via the 'Privacy and Security' link, scrolling to the 'Read the COVIDSafe privacy policy' section and clicking the 'as a web page' hyperlink
- when a user consents to upload their close contacts via the COVIDSafe app, the user is provided a further link to the COVIDSafe Privacy Policy (see paragraph 2.21)
- the COVIDSafe Privacy Policy is available via the COVIDSafe app's website.

3.72 However, as the DTA updated the COVIDSafe app to make the link to the privacy policy accessible from the main screen of the app, no finding or suggestion has been made in relation to this matter.

Key finding: The OAIC is **satisfied** that the COVIDSafe Privacy Policy, meets the requirements of APP 1.5.

APP 5 – notification of the collection of personal information

3.73 APP 5.1 requires an APP entity that collects personal information about an individual to take reasonable steps either to notify the individual of certain matters, or to ensure the individual is aware of those matters, at or before the time of collection, or as soon as reasonably practicable thereafter.

3.74 APP 5.2 lists the matters that must be notified to an individual, or of which they must be made aware (APP 5 matters). For each matter, an APP entity must consider whether notifying the individual is reasonable in the circumstances. The APP 5 matters are:

- the identity and contact information of the APP entity (APP 5.2 (a))
- if the APP entity collects the personal information from someone other than the individual (APP 5.2(b)(i)), or if the individual may not be aware that the APP entity has collected the personal information (APP 5.2(b)(ii)), the fact that the APP collects, or has collected the personal information and the circumstances of the collection
- if the collection of personal information is required, or authorised by or under an Australian law or a court/tribunal, the fact that the collection is so required or authorised (including the name of the Australia law or details of the court / tribunal order authorising collection) (APP 5.2(c))
- the purposes for which the APP entity collects the personal information (APP 5.2(d))
- the main consequences (if any) for the individual if all or some of the personal information is not collected by the APP entity (APP 5.2(e))
- any other APP entity, body or person, or the types of any other APP entities, bodies or persons, to which the APP entity usually discloses personal information of the kind collected by the entity (APP 5.2(f))
- that the APP Privacy Policy of the APP entity contains information about how the individual may access the personal information about the individual that is held by the entity, and seek the correction of that information (APP 5.2(g))
- that the APP Privacy Policy of the APP entity contains information about how the individual may complain about a breach of the APPs, or a registered APP code that binds the entity, and how the entity will deal with such a complaint (APP 5.2(h))
- whether the APP entity is likely to disclose the personal information to overseas recipients (APP 5.2(i)), and if so, the countries in which such recipients are likely to be located (APP 5.2(j)).

3.75 The requirement to notify or ensure awareness of the APP 5 matters applies to all personal information collected about an individual, either directly from the individual or from a third party. It applies to solicited personal information and unsolicited personal information that is not destroyed or de-identified by the APP entity.

3.76 This section examines the COVIDSafe app collection notices as well as the design and technical implementation of the COVIDSafe app against the requirements of APP 5, specifically:

- APP 5.1 - collection notices

- APP 5.2 - APP 5 matters.

3.77 For the purposes of this Assessment, the OAIC had regard to the Chapter 5 of the APP Guidelines, which provide guidance to APP entities on the reasonable steps an APP entity must make to ensure an individual is notified of APP 5 matters or to ensure the individual is aware of those matters.

APP 5.1 - Collection Notices

3.78 An APP entity must take reasonable steps either to notify an individual of the APP 5 matters, or to ensure the individual is aware of those matters (APP 5.1). The reasonable steps for an APP entity will depend upon the circumstances.[12]

3.79 An APP 5 notice may be provided in layers. Brief privacy notices may be supplemented by longer online notices. Where it is not reasonable to notify or ensure awareness of all APP 5 matters, an entity could alert the individual to specific sections of its APP Privacy Policy. However, the entity should consider whether the APP Privacy Policy sufficiently covers the APP 5 matters as they relate to the particular collection. Where an entity directs an individual to APP 5 matters in its APP Privacy Policy, it should in the APP 5 collection notice, make reference to the relevant sections of the privacy policy containing the APP 5 matters.

3.80 The OAIC identified 2 personal information collection practices by the Australian Government in relation to the COVIDSafe app that trigger the APP 5 notification requirement. Those collection practices are:

- the collection of COVID app data in connection with user's registration for, and use of, the COVIDSafe app
- the collection of personal information through a user of the COVIDSafe app requesting the deletion of their personal information held in the NCDS via the 'Request data deletion' Webform.

Collection of COVID app data through COVIDSafe app

3.81 While this is a point in time assessment, in conducting this assessment of whether the collection notices provided meet the requirements of APP 5, the OAIC has reviewed both current and superseded versions of the COVIDSafe app collection notices that the DTA has developed to advise COVIDSafe users of the collection of COVID app data, and the changes to the collection notices and the COVIDSafe System since it was first implemented.

3.82 As identified in the 'Collection' section of this report (see paragraphs 2.9 - 2.19), COVID app data is only collected through the COVIDSafe app. This includes Registration Data, Contact Data and

[12] For a discussion of an APP entity taking reasonable steps to notify or ensure awareness of the APP 5 matters and this being dependant on the circumstances see paragraph 5.4 of the APP Guidelines.

Diagnostic Information. As identified in figure 3, a collection notice is issued when a COVIDSafe user provides their Registration Data in the COVIDSafe app. This collection notice details to users how the Registration Data, Contact Data and Diagnostic Information is collected.

3.83 Similar to the COVIDSafe Privacy Policy, the DTA has, to date, developed 4 versions of the COVIDSafe app collection notice over the lifecycle of the COVIDSafe System. Each version of the collection notice has been updated based on either legislative change or technical changes to the COVIDSafe app. Further detail on these changes is set out in the 'Changes to the COVIDSafe app and COVIDSafe System' section of this assessment report (see paragraphs 2.28 - 2.37).

3.84 The initial version of the collection notice was based on the version of the COVIDSafe app that was developed in accordance with the Biosecurity Determination. This version of the collection notice was issued concurrently with the launch of the COVIDSafe app on 26 April 2020.

3.85 Following the introduction of the Privacy Amendment Act, the collection notice (and COVIDSafe app) was updated to reflect the new legislation. The updated collection notices were released on 9 July 2020.

3.86 The COVIDSafe app collection notice was further updated following introduction of functionality to collect Diagnostic Information. At this time, separate collection notices for iOS and Android devices were developed due to variations in the way these devices operate in relation to the collection of the Diagnostic Information, namely the requirement for Android devices to have location services turned on for Bluetooth to operate. This additional functionality was implemented on 25 September 2020, at which time the collection notices were also updated.

3.87 The OAIC has reviewed the Privacy Assurance Assessment developed in relation to the change to the COVIDSafe app to collect Diagnostic Information, the updated collection notices, the design and technical documentation for the COVIDSafe app and the source code of the COVIDSafe app and is satisfied that the changes to the collection notices as a result of the implementation of this change to collect Diagnostic Information accurately reflect the process by which the Diagnostic Information is collected.

3.88 The introduction of the Herald Bluetooth protocol on 19 December 2020 also resulted in an update to the collection notices. This update was based on a PIA conducted by AGS in November 2020 which found that, although no new or additional personal information was collected, the introduction of the Herald Bluetooth protocol did change the ways in which the personal information may be collected. Therefore, the collection notices were updated to reflect this change on 19 December 2020.

3.89 The OAIC has reviewed the PIA developed by AGS in relation to the introduction of the Herald Bluetooth protocol, the updated collection notices, the design and technical documentation for the COVIDSafe app and the source code of the COVIDSafe app and is satisfied that the changes to the collection notices as a result of the introduction of the Herald Bluetooth protocol accurately reflect the new method for collecting personal information.

3.90 The collection notice is provided just before the time a user provides their Registration Data. The OAIC has reviewed the policy, the design and technical implementation of the COVIDSafe System (including the source code of the COVIDSafe app) and is satisfied that COVIDSafe collection notice is issued just before the time the DTA collects COVID app data.

3.91 The OAIC is satisfied that the DTA has, via the use of the collection notice, taken reasonable steps to inform users of the COVIDSafe app of the collection of their personal information.

Key finding: The OAIC is **satisfied** that the Data Store Administrator is taking reasonable steps to notify individuals of the collection of COVID app data at the time of collection in accordance with APP 5.1.

Variation in the wording in the COVIDSafe Privacy Policy and the collection notices

3.92 The OAIC notes that is has identified a minor variation in the wording used between the COVIDSafe Privacy Policy and the collection notices provided to COVIDSafe users. The COVIDSafe Privacy Policy refers to an 'encrypted user ID', whereas the COVIDSafe app collection notice refers to an 'anonymous ID code'. The DTA advised that the identifier collected by the COVIDSafe app, and exchanged between COVIDSafe users is encrypted, therefore the 'encrypted user ID' is the correct terminology.

3.93 The OAIC considers the variation in the wording between the COVIDSafe Privacy Policy and COVIDSafe app collection notices presents a low privacy risk, as the use of the phrase 'anonymous ID code' in the collection notices may give rise to the perception that an additional type of personal information is collected and exchanged by the COVIDSafe app.

Suggestion 3
The OAIC suggests that the DTA update the terminology used in the collection notices issued to potential COVIDSafe users from 'anonymous' to 'encrypted' to ensure consistency with the COVIDSafe Privacy Policy.

Collection of personal information through 'Request data deletion' Webform

3.94 As identified in the 'Deletion' section of this report (see paragraph 2.26 to 2.27), a COVIDSafe user can request the deletion of their COVID app data stored in the NCDS at any time. To facilitate this process, the DTA has created the 'Request data deletion' Webform (see figure 7).

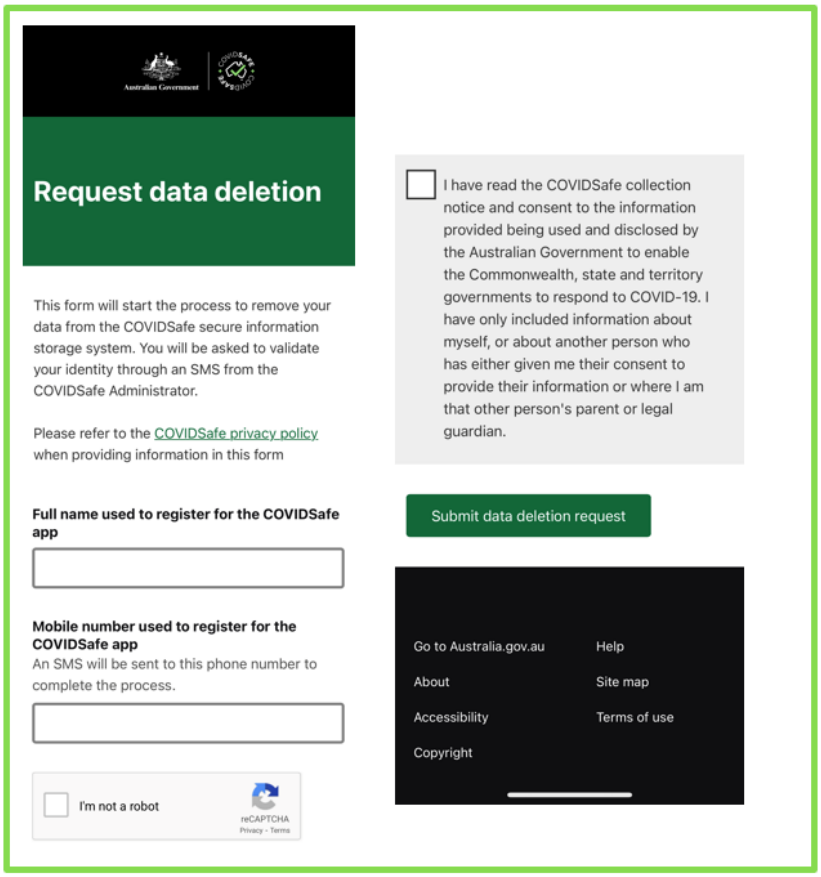


Figure 7 The 'Request data deletion' Webform

3.95 At the time of a request to delete COVID app data from the NCDS, the DTA collects personal information from COVIDSafe users to enable the DTA to identify the relevant COVID app data stored in the NCDS and process its deletion. The personal information collected by the 'Request data deletion' Webform is not considered COVID app data under the definition in s 94D(5) of the Privacy Act, though it will be identical to Registration Data stored in the NCDS. The DTA, during fieldwork interviews, advised that they do not consider the personal information collected via this process to be COVID app data.

3.96 Users who access the 'Request data deletion' Webform are

- referred via a link on this Webform to the COVIDSafe Privacy Policy, and
- asked to indicate they have read the COVIDSafe app collection notice and consent to the use of the personal information to allow the Commonwealth, State and Territory governments to respond to COVID-19.

3.97 The COVIDSafe Privacy Policy, under the heading 'How will personal information be used and disclosed?' includes information about use or disclosure of personal information 'to confirm that the correct data is being deleted', when a COVIDSafe user makes 'a request to delete personal information held in the data store'. This is referring to the process whereby the DTA identifies the COVID app data to be deleted from the NCDS by using the mobile phone number

that the DTA has collected via the Request data deletion' Webform. The COVIDSafe Privacy Policy and collection notices refer to the collection of COVID app data and do not refer to the collection of personal information via the 'Request data deletion' Webform.

3.98 The OAIC considers a medium privacy risk exists that COVIDSafe users are not, in the context that they access the 'Request data deletion' Webform, appropriately notified of the purposes for the collection, and management, of personal information collected via the webform as required under APP 5.1. To address compliance with the requirements of APP 5.1, the OAIC recommends that the DTA develop a dedicated collection notice for the 'Request data deletion' Webform. This collection notice will make individuals aware of the APP 5 matters (discussed from paragraph 3.99 onwards below) at the time and in the context of the DTA collecting individuals' personal information in connection with a request to have their data deleted from the NCDS. The DTA should clearly and prominently display the APP 5 matters in the 'Request data deletion' Webform, or consider other layered ways to display APP 5 matters if it is not practical to include in the webform all the necessary APP 5 matters, such as a prominent link to a detailed APP 5 notice from this webform or a popup box which automatically appears when users fill out the form. Alternately, the DTA could:

- alert individuals to specific sections of its updated APP Privacy Policy. However, before doing so the DTA should consider whether information in the APP Privacy Policy sufficiently covers the APP 5 matters as they relate to the particular collection of personal information via the Request data deletion' Webform, and
- include a link on the webform to the updated APP Privacy Policy alerting individuals to the relevant sections of its APP Privacy Policy in the webform.

Recommendation 1

The OAIC recommends that the DTA develop and issue a collection notice for the 'Request data deletion' Webform in accordance with APP 5.1. Alternately, the DTA could:

- alert individuals to specific sections of its updated APP Privacy Policy. However, before doing so the DTA should consider whether information in the APP Privacy Policy sufficiently covers the APP 5 matters in relation to the particular collection and use of personal information via the 'Request data deletion' Webform to facilitate the deletion of COVID app data, and
- direct COVIDSafe users accessing the 'Request data deletion' Webform to the relevant sections of the updated APP Privacy Policy.

APP 5.2 - APP 5 matters

3.99 APP 5.2 outlines the APP matters an APP entity is required to include when notifying an individual of the collection of personal information. For each of the APP 5 matters, an APP entity must consider whether notifying an individual about that matter is reasonable. This means it may be reasonable for an entity to notify, some, but not all, of the APP 5 matters.

'Request data deletion' webform compliance with APP 5.2

3.100 As identified in paragraph 3.96, during the collection of personal information related to the 'Request data deletion' Webform, COVIDSafe users are currently directed to the COVIDSafe app collection notices, which the OAIC does not consider to be appropriate collection notices under APP 5 for the purposes of collecting personal information from individuals requesting deletion of their COVID app data from the NCDS. Given this, the collection notice for the collection of personal information associated with the 'Request data deletion' Webform is not compliant with the requirements of APP 5.2. The OAIC recommends that the DTA prepare a collection notice for the 'Request data deletion webform' in accordance with the requirements of APP 5.2.

Recommendation 2
The OAIC recommends that the DTA, in relation to the collection of personal information via the 'Request data deletion' Webform, take reasonable steps to notify individuals or ensure their awareness of the APP 5 matters is in accordance with the requirements in APP 5.2.

The APP entity's identity and contact details (APP 5.2(a))

3.101 APP 5.2(a) requires APP entities to set out the identity and contact details of the APP entity collecting an individual's information in any collection notice provided to them. This could include the position title, telephone number and email address of a contact who handles enquiries and requests relating to the Privacy Act.

3.102 The OAIC notes that:

- the COVIDSafe app collection notice (figure 3) does not identify the DTA as the entity collecting the personal information and provide their contact details
- the DTA is identified as the entity collecting the personal information in the 'Registration consent' screen which directly follows the collection notice (see figure 4)
- the identity of and contact information for the DTA is provided in the COVIDSafe Privacy Policy that is linked in the COVIDSafe app collection notice (see figure 3).

3.103 In relation to the matters to be set out in APP5.2(a), the OAIC is satisfied that the COVIDSafe app collection notice provides sufficient information to meet the requirements of APP 5.2(a) as the COVIDSafe Privacy Policy and 'Registration consent' screen identify the DTA. However, the OAIC

considers there to be a low privacy risk associated with the COVIDSafe app collection notice not directing individuals to the section of the COVIDSafe Privacy Policy which contains the identity and contact details of the DTA. Therefore, the OAIC suggests that the collection notice, is amended to identify the section of the COVIDSafe Privacy Policy which contains the identity and contact details of the DTA.

Suggestion 4
The OAIC suggests that the DTA revise the COVIDSafe app collection notice to direct individuals to the section of the COVIDSafe Privacy Policy that sets out the identity and contact details of the DTA as the entity collecting the personal information.

The facts and circumstances of collection (APP 5.2(b))

3.104 APP 5.2(b) requires a collection notice to set out the facts and circumstances of collection. This may include how, when and from where (including third parties) the personal information was collected.

3.105 Where an individual may not be aware of their personal information being collected (e.g. as a result of the COVIDSafe app collecting Diagnostic Information), the individual should be made aware of the method of collection.

3.106 The OAIC notes that the COVIDSafe app collection notice provides COVIDSafe users with the details of the Registration Data, Contact Data and Diagnostic Information collected and provides a high-level overview of how and when the information is collected, including that their Contact Data may be collected by other COVIDSafe users and provided to a STHA.

3.107 The OAIC is satisfied that the COVIDSafe app collection notice provides sufficient information to users of the COVIDSafe app regarding the facts and circumstances of collection of their personal information to satisfy APP 5.2(b).

If the collection is required or authorised by law (APP 5.2(c))

3.108 APP 5.2(c) requires that the APP entity outline whether (if applicable) the collection is required or authorised by or under an Australian law or a court/tribunal order.

3.109 The COVIDSafe app collection notice advises users that the use of the COVIDSafe app is voluntary and that they can install or delete the COVIDSafe app at any time and provides a link to request the deletion of COVID app data collected.

3.110 Collection, use and disclosure of personal information by the COVIDSafe app is authorised by s 94D(2) of the Privacy Act. The collection notice states that COVIDSafe will collect, use or disclose an individual's personal information 'only in accordance with this policy and the Privacy Act'. The OAIC notes that the COVIDSafe Privacy Policy that is linked in the COVIDSafe

app collection notice (see figure 3) refers to how personal information that is collected via the COVIDSafe app will be handled in accordance with the Privacy Act. The COVIDSafe Privacy Policy provides further information in relation to the amendments to the Privacy Act made by the Privacy Amendment Act, which 'provide stronger privacy protections for users of the COVIDSafe App and information collected through the App'. The fact that the collection of COVID app data is 'authorised' by the Privacy Act may be implied from these references in the collection notice and COVIDSafe Privacy Policy. The OAIC considers there to be a low privacy risk associated with the COVIDSafe app collection notice not expressly stating that the collection is 'authorised' by the Privacy Act, noting that the collection notice provides a link to the COVIDSafe Privacy Policy which also does not expressly state that the collection is authorised by the Privacy Act.

3.111 Therefore, the OAIC suggests that either:

- the collection notice, is amended to expressly state that the collection of personal information is authorised by the Privacy Act, or
- the COVIDSafe Privacy Policy is amended to expressly state that the collection of personal information is authorised by the Privacy Act and the collection notice is amended to reference this section of the privacy policy.

Suggestion 5
The OAIC suggests that the DTA amend the COVIDSafe app collection notice to expressly state that the collection of personal information is authorised by the Privacy Act, or the COVIDSafe Privacy Policy is amended to expressly state that the collection of personal information is authorised by the Privacy Act and the collection notice is amended to reference this section of the policy.

The purposes of collection (APP 5.2(d))

3.112 APP 5.2(d) requires that the APP entity outline the purposes for which the APP entity collects the personal information. This includes the primary purpose of collection, that is, the specific function or activity for which particular personal information is collected. If the APP entity may use or disclose personal information for purposes other than the primary purpose (known as a 'secondary purpose'), these could also be included.

3.113 The COVIDSafe app collection notice advises COVIDSafe users that COVID app data will be used or disclosed for contact tracing purposes and to ensure the proper and lawful functioning of the COVIDSafe app. The OAIC notes further detail regarding the collection and use of personal information by the COVIDSafe app is set out in the COVIDSafe Privacy Policy.

3.114 The OAIC is satisfied that the COVIDSafe app collection notice adequately details the primary purposes for which personal information is collected, and provides reasonable detail to users

as to secondary uses of personal information (e.g. ensuring the lawful function of the COVIDSafe app).

The consequences for the individual if personal information is not collected (APP 5.2(e))

3.115 APP 5.2(e) requires that the APP entity outline the main consequences (if any) for the individual if all or some of the personal information is not collected by the APP entity. An APP entity is not required to list all possible or remote consequences or those that would be obvious to a reasonable person. Instead, it should describe significant consequences that could be expected to result.

3.116 As identified in paragraph 3.109, the use of the COVIDSafe app is completely voluntary. The COVIDSafe app collection notice advises users of this, however the OAIC notes the collection notice does not explicitly state that the COVIDSafe app is unable to function unless a user provides their personal information.

3.117 The OAIC considers there to be a low privacy risk associated with the COVIDSafe app collection notice not explicitly stating that the user must provide their personal information in order for the COVIDSafe app to function.

Suggestion 6
The OAIC suggests that the DTA revise the collection notice to explicitly state that, whilst use of the COVIDSafe app is entirely voluntary, the COVIDSafe app is unable to function unless a user provides the requested personal information.

Other APP entities, bodies or persons to which the personal information is usually disclosed (APP 5.2(f))

3.118 The matters set out in APP 5.2(f) to be included in a collection notice is the details of any other APP entity, body or person, or the types of other APP entities, bodies or persons, to which the APP entity usually discloses personal information of the kind collected by the entity.

3.119 The COVIDSafe app collection notice advises that COVID app data will only be used or disclosed for contact tracing purposes and to ensure the proper and lawful functioning of the COVIDSafe app. This includes that the information may be disclosed to a STHA official.

3.120 The OAIC is satisfied that the COVIDSafe app collection notice provides the details of any other APP entity, body or person, or the types of other APP entities, bodies or persons, to which the APP entity usually discloses personal information of the kind collected by the entity.

Information about access and correction in the APP entity's APP Privacy Policy (APP 5.2(g)) and complaints (APP 5.2(h))

3.121 The matters set out in APP 5.2(g) and (h) to be included in a collection notice are that the APP entity's APP privacy policy contains information about how the individual may:

- access and seek correction of their personal information held by the entity (APP 5.2(g))
- complain to the entity about a breach of the APPs, or any registered APP code that binds the entity, and how the entity will deal with such a complaint (APP 5.2(h)).

3.122 The COVIDSafe app collection notice provides links to the COVIDSafe Privacy Policy and directs COVIDSafe users to access the COVIDSafe Privacy Policy for further details about users' rights. The COVIDSafe Privacy Policy describes the process for correcting COVID app data and making a complaint to the DTA, OAIC or Australian Federal Police.

3.123 As noted above, s 94D(2) of the Privacy Act prevents the DTA from providing COVIDSafe users with access to their COVID app data. The COVIDSafe Privacy Policy advises users that they cannot access their 'data held in the data store', which is COVID app data. A low privacy risk has been identified in relation to this (see Suggestion 2).

3.124 The OAIC is satisfied that the COVIDSafe app collection notice provides sufficient detail to COVIDSafe users that the COVIDSafe Privacy Policy contains information about how they can (subject to the applicable limitations in s 94D(2) of the Privacy Act) seek correction of their personal information and complain to the entity about a breach of the APPs, or any registered APP code that binds the entity, and how the entity will deal with such a complaint.

Likely cross-border disclosures of the personal information (APP 5.2(i) and (j))

3.125 The matters set out in APP 5.2(i) and (j) to be included in a collection notice are:

- whether the APP entity is likely to disclose the personal information to overseas recipients (APP 5.2(i))
- if so, the countries in which such recipients are likely to be located if it is practicable to specify those counties in the notice or to otherwise make the individual aware of them (APP 5.2(j)).

3.126 This requirement only applies to a likely disclosure of personal information to an overseas recipient. It does not apply to a use of personal information by an APP entity that does not constitute a disclosure.

3.127 Pursuant to s 94F of the Privacy Act, it is an offence for COVID app data to be held on a database outside Australia and for a person to disclose COVID app data to a person overseas. The NCDS is hosted by AWS and the DTA has determined that COVID app data in the NCDS will only be

stored in Australia. Further information relating to the compliance of the DTA, as the DSA, in relation to s 94F is provided in COVIDSafe Assessment 1.

3.128 As it is an offence for COVID app data to be held on a database outside Australia and the DTA has determined that COVID app data in the NCDS will only be stored in Australia, the OAIC is satisfied that APP 5.2(i) and 5.2(j) are not applicable matters to be detailed in the COVIDSafe app collection notice.

Key finding: The OAIC is **satisfied** that the COVIDSafe app collection notices include the applicable APP 5 Matters and meets the requirements of APP 5.2.

Part VIIIA of the Privacy Act

3.129 Part VIIIA of the Privacy Act provides additional privacy protections for personal information collected through the COVIDSafe app.

3.130 This section examines the design and technical implementation of the COVIDSafe app, the NCDS and the HOP for compliance with Part VIIIA of the Privacy Act, specifically:

- section 94D – collection, use or disclosure of COVID app data
- section 94E – COVID app data on communication devices
- section 94F – COVID app data in the National COVIDSafe Data Store
- section 94G – Decrypting COVID app data.

3.131 Elements of the NCDS were considered as part of COVIDSafe Assessment 1 and the HOP was considered as part of COVIDSafe Assessment 2[13]. The NCDS and HOP have again been considered as part of this privacy assessment to ensure that elements of the NCDS and HOP, as they relate to the compliance of the COVIDSafe Privacy Policy and collection notices with the applicable APP requirements, have been appropriately assessed.

3.132 As identified in paragraph 3.96, the DTA may collect personal information that is identical to COVID app data via the 'Request data deletion' Webform, however such information is not considered COVID app data under the definition provided in s 94D(5) of the Privacy Act.

3.133 As this data is not considered COVID app data, the requirements of Part VIIIA of the Privacy Act do not apply and therefore the collection, use and disclosure of this personal information via the 'Request data deletion' Webform is outside the scope of this assessment.

[13] At the time of publication of this assessment report, COVIDSafe Assessment 2 was not finalized.

3.134 To assess compliance of the DSA with ss 94D, 94E, 94F and 94G of the Privacy Act the OAIC reviewed:

- the COVIDSafe Privacy Policy and collection notices
- the design and technical implementation of the COVIDSafe app
- the source code of the COVIDSafe app.

3.135 In addition, the OAIC conducted interviews with key DoH and DTA staff.

Section 94D – collection, use or disclosure of COVID app data

3.136 As outlined in paragraph 3.58, s 94D of the Privacy Act makes it an offence to collect, use or disclose data that is COVID app data except for the permitted purposes set out in s 94D(2) of the Privacy Act.

3.137 The OAIC found that the description of the collection, use and disclosure of COVID app data set out in the COVIDSafe Privacy Policy and collection notices accords with the requirements s 94D of the Privacy Act.

3.138 Further, the OAIC reviewed the technical operation of the COVIDSafe app relating to the collection, use and disclosure of COVID app data to determine whether the collection and use of COVID app data, and its disclosure to the NCDS, is done so in accordance with the requirements of s 94D. In assessing the compliance of the COVIDSafe app, the OAIC reviewed the source code of the app, available via GitHub, and reviewed relevant technical forums, expert opinion and criticism of the COVIDSafe app.

3.139 On the basis of the documentation reviewed, the source code of the COVIDSafe app and the key DoH and DTA staff interviewed, the OAIC is satisfied that the collection, use and disclosure of COVID app data by the COVIDSafe app, NCDS and HOP (collectively the COVIDSafe System) complies with s 94D of Part VIIIA of the Privacy Act.

3.140 Further information relating to the compliance of the DTA, as the DSA, in relation to the NCDS and compliance with s 94D is provided in COVIDSafe Assessment 1.

Key finding: On the basis of this point in time assessment, the OAIC is **satisfied** that the COVIDSafe System and Data Store Administrator are complying with s 94D in relation to the collection, use or disclosure of COVID app data.

Section 94E – COVID app data on communication devices

3.141 Section 94E of the Privacy Act makes it an offence to upload, or cause to be uploaded, COVID app data to the NCDS unless consent from the COVIDSafe user or their parent, guardian or carer (if applicable) has been obtained.

3.142 Consent is defined in s 6(1) of the Privacy Act and means 'express consent or implied consent'. The 4 key elements of consent are:

- the individual is adequately informed before giving consent
- the individual gives consent voluntarily
- the consent is current and specific, and
- the individual has the capacity to understand and communicate their consent.

3.143 As outlined in paragraphs 2.20 – 2.25 and figure 6, the DTA has implemented a process whereby the consent of the COVIDSafe user, or their parent, guardian or carer, and the input of public health official, with access to the HOP, are required in order to facilitate the upload of COVID app data from a COVIDSafe user's communication device to the NCDS.

3.144 The OAIC's found a COVIDSafe user cannot upload their Contact Data without an official first generating a 6-digit PIN through the HOP. Similarly, a STHA official can only request a COVIDSafe user to upload their Contact Data and requires the COVIDSafe user to consent prior to the upload to the NCDS commencing. COVID app data will not be uploaded to the NCDS without this consent.

3.145 The COVIDSafe user can choose not to upload their data at any point until they have entered the PIN provided by the STHA official. Contact Data that are considered COVID app data are only stored on a communication device for a period of 21 days and can only be uploaded following the method described above.

3.146 On the basis of the documentation reviewed, the source code of the COVIDSafe app and the key DoH and DTA staff interviewed, the OAIC is satisfied that the functionality implemented to COVIDSafe app and the HOP, only allows for COVID app data to be uploaded following consent being obtained from the COVIDSafe user, and that this consent is actively sought and informed prior to any upload, in compliance with s 94E of Part VIIIA of the Privacy Act.

Key finding: On the basis of this point in time assessment, the OAIC is **satisfied** that the DSA is complying with s 94E in relation to COVID app data on communication devices.

Section 94F – COVID app data in the National COVIDSafe Data Store

3.147 Section 94F(1) of the Privacy Act makes it an offence for any person to retain data on a database outside of Australia and that data is COVID app data that has been uploaded from a communication device to the NCDS. Section 94F(2) also makes it an offence for any person to disclose data to another person who is outside of Australia and that data is COVID app data that

has been uploaded from a communication device to the NCDS, where that person is not employed by a STHA for the purposes of undertaking contact tracing.

3.148 Section 94F of the Privacy Act applies to COVID app data that has been uploaded to the NCDS, but not COVID app data that is retained on a communication device.

3.149 Further information of the DTA's compliance with s 94F in respect of COVID app data uploaded to the NCDS has been considered in COVIDSafe Assessment 1.

Section 94G – decrypting COVID app data

3.150 Section 94G of the Privacy Act outlines that it is an offence to decrypt COVID app data that is stored on a communications device.

3.151 The encryption used by the DTA to secure COVID app data has been assessed by the Australian Cyber Security Centre (ACSC). Further information on the encryption method used by the DTA is provided in COVIDSafe Assessment 1.[14]

3.152 Following registration, the COVIDSafe user's encrypted ID will be stored on their communication device and exchanged with other COVIDSafe users when they are within range (1.5 metres) as part of the Contact Data. Contact Data that has been exchanged with other COVIDSafe users' devices will be deleted from their device after 21 days on a rolling basis.

3.153 On the basis of the documentation reviewed, the source code of the COVIDSafe app and the key DoH and DTA staff interviewed, the OAIC is satisfied that in relation to the COVIDSafe app, COVID app data has not been decrypted, except where permitted, in compliance with s 94G of the Privacy Act.

Key finding: On the basis of this point in time assessment, the OAIC is **satisfied** that s 94G is being complied with by the Data Store Administrator in relation to the decryption of COVID app data.

[14] In undertaking fieldwork for Assessment 1, the OAIC found that the ACSC provided advice to the DTA in relation to the implementation of the encryption. Both encryption in transit and platform-level encryption of the NCDS (encryption at rest) protect COVID app data.

Part 4: Recommendations, suggestions and responses

Recommendation 1

OAIC Recommendation

4.1 The OAIC recommends that the DTA develop and issue a collection notice for the 'Request data deletion' Webform in accordance with APP 5.1. Alternately, the DTA could

- alert individuals to specific sections of its updated APP Privacy Policy. However, before doing so the DTA should consider whether information in the APP Privacy Policy sufficiently covers the APP 5 matters in relation to the particular collection and use of personal information via the 'Request data deletion' Webform to facilitate the deletion of COVID app data, and
- direct COVIDSafe users accessing the 'Request data deletion' Webform to the relevant sections of the updated APP Privacy Policy.

DoH response to the recommendation[15]

4.2 Agreed. The Department of Health (DoH) will review its existing APP Privacy Policy to ensure it sufficiently cover APP 5 matters related to the collection and use of personal information collected by the 'request data deletion' Webform. DoH will ensure that the link to access the APP Privacy Policy is available to those using the 'request data deletion' Webform.

Recommendation 2

OAIC Recommendation

4.3 The OAIC recommends that the DTA, in relation to the collection of personal information via the 'Request data deletion' Webform, take reasonable steps to notify individuals or ensure their awareness of the APP 5 matters is in accordance with the requirements in APP 5.2.

DoH response to the recommendation

4.4 Agreed. DoH will take reasonable steps to notify individuals using the 'request data deletion' Webform have access to the modified APP Privacy Policy per Recommendation 1. The modified APP Privacy Policy will address the requirements of APP 5.2.

[15] At the time of consultation for this assessment report, the responsibility for the administration of the COVIDSafe app and NCDS was being transitioned from the DTA to the DoH. Consequently, the DoH responded on behalf of both entities.

Suggestion 1

OAIC suggestion

4.5 The OAIC suggests the DTA update the COVIDSafe Privacy Policy with a brief explanation of how the encrypted user ID is created and assigned to each user.

DoH response to the suggestion

4.6 Agreed. DoH will update the COVIDSafe Privacy Policy with an explanation as to how the encrypted user ID is created and assigned to each user.

Suggestion 2

OAIC suggestion

4.7 The OAIC suggests that the DTA update the COVIDSafe Privacy Policy to advise COVIDSafe users that access to their COVID app data is not permitted by law.

DoH response to the suggestion

4.8 Agreed. DoH will update the COVIDSafe Privacy Policy to advise users of the COVIDSafe App that access to their COVID data is not permitted by law.

Suggestion 3

OAIC suggestion

4.9 The OAIC suggests that the DTA update the terminology used in the collection notices issued to potential COVIDSafe users from ‘anonymous’ to ‘encrypted’ to ensure consistency with the COVIDSafe Privacy Policy.

DoH response to the suggestion

4.10 Agreed. DoH will change the terminology used in the collection notice from ‘anonymous’ to ‘encrypted’ to align with the COVIDSafe Privacy Policy.

Suggestion 4

OAIC suggestion

4.11 The OAIC suggests that the DTA revise the COVIDSafe app collection notice to direct individuals to the section of the COVIDSafe Privacy Policy that sets out the identity and contact details of the DTA as the entity collecting the personal information.

DoH response to the suggestion

4.12 Agreed. DoH will ensure that the COVIDSafe app collection notice informs users that there is a COVIDSafe Privacy Policy. DoH will also ensure that the COVIDSafe Privacy Policy identifies the DoH as the entity collecting the personal information.

Suggestion 5

OAIC suggestion

4.13 The OAIC suggests that the DTA amend the COVIDSafe app collection notice to expressly state that the collection of personal information is authorised by the Privacy Act, or the COVIDSafe Privacy Policy is amended to expressly state that the collection of personal information is authorised by the Privacy Act and the collection notice is amended to reference this section of the policy.

DoH response to the suggestion

4.14 Agreed. DoH will amend the COVIDSafe Privacy Policy to state that the collection of personal information is authorised by the Privacy Act.

Suggestion 6

OAIC suggestion

4.15 The OAIC suggests that the DTA revise the collection notice to explicitly state that, whilst use of the COVIDSafe app is entirely voluntary, the COVIDSafe app is unable to function unless a user provides the requested personal information.

DoH response to the suggestion

4.16 Agreed. DoH will modify the collection notice to inform users that the COVIDSafe app is unable to function unless the user provides the requested personal information. The COVIDSafe collection notice already states that the use of the COVIDSafe app is voluntary.

Part 5: Description of assessment

Objective and scope of assessment

5.1 This assessment was conducted under Part VIIIA of the Privacy Act, which legislates oversight for the COVIDSafe System by the AIC.

5.2 The objective of this assessment was to determine whether the functionality of the COVIDSafe system meets the specified privacy protections as set out under the COVIDSafe Privacy Policy and collection notices in compliance with APPs 1.3, 1.4, 1.5, APP 5 and Part VIIIA of the Privacy Act in the time period from April to December 2020.

5.3 In order to form a conclusion against Assessment 3 objectives, the following criteria were examined:

- the COVIDSafe Privacy Policy and Collection Notices for compliance with APP 1 and APP 5
- the design and technical implementation of the COVIDSafe app, the HOP and the NCDS for alignment to the COVIDSafe Privacy Policy, collection notices and recommendations outlined in the PIA
- the COVIDSafe app, HOP and NCDS for compliance with the collection, disclosure and retention requirements of Part VIIIA of the Privacy Act.

5.4 The OAIC determined the approach undertaken in conducting Assessment 3, referring to reporting requirements as legislated in the Privacy Act. The PwC Global Internal Audit Methodology aligned with the requirements of the International Professional Practices Framework was also referenced to provide further assurance.

Privacy risks

5.5 Where the OAIC identified privacy risks and considered those risks to be low risks, the OAIC made suggestions about how to address those risks. These observations are set out in Part 3 of this report.

5.6 The OAIC assessments are conducted as a 'point in time' assessment i.e. observations are only applicable to the time period in which the assessment was undertaken.

5.7 For more information about OAIC privacy risk ratings, refer to the OAIC's 'Risk based assessments – privacy risk guidance'. Chapter 7 of the OAIC's Guide to privacy regulatory action provides further detail on this approach.

5.8 Assessment 3 provides assurance that the DTA and DoH are effectively managing the following specific risks as noted in the DoH COVIDSafe app PIA:

1. Insufficient assurance is provided to the Australian people about the function and purpose of the COVIDSafe app, how the app will work, what personal information will be collected by the app, and how that information will be used.
2. 'Data minimisation principle' is not observed, so that the amount of personal information collected is more than required.
3. Consent is not appropriately obtained or provided where users of the COVIDSafe app do not properly understand how their personal information will be handled.
4. Appropriate consent is not obtained from parents/guardians for users who are children under the age of 16.
5. COVID app data is not secure.
6. Data governance arrangements (outlined in contracts and other arrangements) between entities involved in the implementation and operation of the COVIDSafe app are insufficient to secure, and appropriately monitor, access to COVID app data.

Timing, location and assessment techniques

5.9 The OAIC conducted both a risk-based assessment of the functionality of the COVIDSafe system under APP 1 and APP 5 which focused on identifying privacy risks to the secure handling of COVID app data and a compliance-based assessment under Part VIIIA of the Privacy Act.

5.10 Assessment 3 involved the following activities:

- review of relevant policies, procedures, design and technical documentation provided by the DoH and the DTA
- a review of the COVIDSafe app source code, including a review of the source code published to GitHub and public discussion forums and expert opinion on the source code
- fieldwork, which included interviewing key members of staff at the DTA and the DoH offices in Canberra during November and December 2020.

5.11 The OAIC engaged PwC to assist with undertaking the COVIDSafe Assessment Program to provide independent assurance to Australian citizens that data in the COVIDSafe app is meeting legislative requirements. The OAIC considered PwC observations in the writing of this report.

Reporting

5.12 The OAIC publishes final assessment reports in full, or if necessary, an abridged version, on its website. All or part of an assessment report may be withheld from publication due to statutory secrecy provisions, privacy, confidentiality, security or privilege.

Appendix A: COVIDSafe Legislative Framework

COVIDSafe Legislative Framework

1.1 The personal information collected by the COVIDSafe app through the COVIDSafe System is protected by the following:

- The *Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements—Public Health Contact Information) Determination 2020* (Cth) (the **Biosecurity Determination**)
- The Privacy Act, which includes:
    - The APPs
    - Part VIIIA – Public health contact information.

The Biosecurity Determination

1.2 The Biosecurity Determination was issued by the Minister for Health on 25 April 2020 under the *Biosecurity Act 2015* (Cth) and was repealed on 16 May 2020 following commencement of the *Privacy Amendment (Public Health Contact Information) Act 2020* (Cth) (Privacy Amendment Act).

1.3 The Biosecurity Determination included requirements for the collection, use and disclosure of COVID app data and was regulated by the Australian Federal Police, not the OAIC.

Privacy Act – the Australian Privacy Principles

1.4 The Privacy Act promotes and protects the privacy of individuals and regulates how APP entities, which includes Australian Government agencies and organisations, handle personal information.

1.5 The APPs at Schedule 1 of the Privacy Act are the cornerstone of the privacy protection framework in the Act. The 13 APPs govern standards, rights and obligations around:

- the collection, use and disclosure of personal information
- an organisation or agency's privacy governance and accountability
- the integrity and correction of personal information
- the rights of individuals to access their personal information.

1.6 The APPs apply to any 'personal information' collected by Australian Government agencies in relation to the COVIDSafe System.

Privacy Amendment (Public Health Contact Information) Act 2020 (Privacy Amendment Act) and Part VIIIA of the Privacy Act

1.7 The Australian Government passed the Privacy Amendment Act on 14 May 2020 which amended the Privacy Act by inserting *Part VIIIA – Public health contact information* into the Privacy Act. Part VIIIA commenced on 16 May 2020.

1.8 Part VIIIA of the Privacy Act provides strong privacy protections for personal information collected through the COVIDSafe app. The Australian Information Commissioner (AIC) has an independent oversight function in relation to COVIDSafe under the Privacy Act and is actively monitoring and regulating compliance.

1.9 Specific privacy protections under Part VIIIA include:

- section 94D: collection, use and disclosure of COVID app data
- section 94E: COVID app data on communication devices
- section 94F: COVID app data in the NCDS
- section 94G: decrypting COVID app data.

1.10 The provisions dealing with privacy protection are supported by procedural amendments which relate to or assist with oversight of the COVIDSafe System by the OAIC, including:

- section 94T: expands the assessment power in s 33C to include assessments of whether the acts or practices of an entity or a STHA in relation to COVIDSafe data comply with Part VIIIA of the Privacy Act
- section 94Y: provides the Minister for Health with the power to determine, by notifiable instrument, the end of the COVIDSafe data period
- section 94ZB: requires the AIC to report on the performance of their functions and powers relating to Part VIIIA of the Privacy Act every 6 months
- section 94ZC: provides that COVIDSafe data remains the property of the Commonwealth even after disclosure to and use by STHA.

Appendix B: Role of the OAIC

1.1 The new Part VIIIA of the Privacy Act has granted the AIC a range of additional proactive and reactive regulatory powers which support the AIC's legislated responsibilities in relation to the privacy oversight of the COVIDSafe System.

1.2 The OAIC is undertaking 5 privacy assessments (the COVIDSafe Assessment Program) under s 33C and s 94T of the Privacy Act to proactively execute its oversight function in relation to the COVIDSafe System.

1.3 The 5 COVIDSafe privacy assessments (COVIDSafe Assessment Program) are:

- Assessment 1 – Access controls applied to the Data Store by the DSA
- Assessment 2 – Access controls applied to the use of COVID app data by State or Territory Health Authorities
- Assessment 3 – Functionality of the COVIDSafe app against specified privacy protections set out under the COVIDSafe privacy policy and collection notices, and against the requirements of Part VIIIA
- Assessment 4 – Compliance of the DSA with data handling, retention and deletion requirements under Part VIIIA
- Assessment 5 – Compliance of the DSA with the deletion and notification requirements in Part VIIIA which relate to the end of the pandemic.

1.4 Each COVIDSafe Assessment targets different components of the COVIDSafe System, with the COVIDSafe Assessment Program designed to collectively follow the 'information lifecycle' of personal information collected by the Australian Government's COVIDSafe app.

1.5 In undertaking the COVIDSafe Assessment Program, the OAIC seeks to provide independent assurance to Australians that personal information in the COVIDSafe app is being handled in accordance with Part VIIIA and the APPs.

Appendix C: Control Frameworks and Control Measures

The following Control Frameworks and Control Measures have been identified and have been used as the basis for testing in this Assessment:

Legislative framework

Privacy Act

The Privacy Act was introduced to promote and protect the privacy of individuals and to regulate how Australian Government agencies and organisations with an annual turnover of more than $3 million, and some other organisations, handle personal information. For the purpose of these assessments the following aspects of the of the Privacy Act were applied:

- APPs: The APPs are the cornerstone of the privacy protection framework in the Privacy Act. They apply to any organisation or agency the Privacy Act covers. The following APPs were referenced in Assessment 3:
    - APP 1 – Open and transparent management of personal information:
        - Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.
    - APP 5 – Notification of the collection of personal information:
        - Outlines when and in what circumstances an APP entity that collects personal information must tell an individual about certain matters.
- Notifiable Data Breaches: A data breach happens when personal information is accessed or disclosed without authorisation or is lost. If the Privacy Act covers an organisation or agency, that organisation or agency must notify affected individuals and the OAIC when a data breach involving personal information is likely to result in serious harm.
- Part VIIIA: The Privacy Act was amended on 14 May 2020 to protect data in the COVIDSafe app and the NCDS. In relation to the design and technical implementation of the COVIDSafe app, the HOP and the NCDS, the relevant provisions of Part VIIIA of the Privacy Act that were examined in this assessment were:
    - the collection of COVID app data (s 94D)
    - the circumstances in which COVID app data is uploaded to the NCDS to ensure it is only uploaded after the consent of the COVIDSafe user or their parent, guardian or carer (if applicable) has been obtained (s 94E)

Legislative framework

- compliance with the requirement to not retain on a database outside of Australia COVID app data that has been uploaded from a communications device to the NCDS (s 94F)
- compliance with the requirement to not decrypt COVID app data stored on a communications device (s 94G).

Control Framework

Protective Security Policy Framework

The Protective Security Policy Framework (PSPF) assists Australian Government entities to protect their people, information and assets, both at home and overseas. It sets out government protective security policy and supports entities to effectively implement the policy across security governance, information security, personnel, security, physical security.

The Information Security domain was applied in the Assessment program. Specifically, the following core requirements were referenced:[16]

- Policy 8 – Sensitive and security classified information:
  - COVIDSafe app information holdings are identified
  - Sensitivity and security classification of information holdings are assessed
  - Operational controls proportional to value, importance and sensitivity are implemented and managed effectively
- Policy 9 – Access to information:
  - Information is shared appropriately within DTA/DoH as well as with other relevant personnel i.e. STHA personnel
  - Personnel who access sensitive or security classified information have appropriate security clearance and need to know that information
  - Controlling STHA access (including remote access) to supporting COVIDSafe systems, networks, infrastructure, devices and applications is implemented and managed effectively
- Policy 10 – Safeguarding information from cyber threats:

[16] Supporting requirements will be referenced as necessary.

Control Framework

- Core mitigation strategies are implemented and managed effectively across:
  - application controls
  - restricting administrative privileges
- Additional mitigation strategies to protect COVID app data are implemented

- Policy 11 – Robust ICT systems:
  - The Australian Information Security Manual's cyber security principles are applied during all stages of the lifecycle of each COVIDSafe System to ensure the secure operation of ICT systems, safeguard COVID app data and to continuously deliver COVIDSafe app services

Information Security Manual

The Australian Government Information Security Manual (ISM) is a cyber security framework that organisations can apply, using their risk management framework, to protect their systems and information from cyber threats.

The 'govern, protect and detect' activities will be applied in the Assessment program. Specifically, the following principles were referenced:

- G2: The identity and value of systems, applications and data is determined and documented
- G3: The confidentiality, integrity and availability requirements of systems, applications and information is determined and documented
- G4: Security risk management processes are embedded into organisational risk management frameworks
- G5: Security risks are identified, documented, managed and accepted both before systems and applications are authorised for use, and continuously throughout their operational life
- P1: Systems and applications are designed, deployed, maintained and decommissioned according to their value and their confidentiality, integrity and availability requirements
- P2: Systems and applications are delivered and supported by trusted suppliers
- P3: Systems and applications are configured to reduce their attack surface
- P4: Systems and applications are administered in a secure, accountable and auditable manner

Control Framework
• P5: Security vulnerabilities in systems and applications are identified and mitigated in a timely manner • P6: Only trusted and supported operating systems, applications and computer code can execute on systems • P8: Information communicated between different systems is controlled, inspectable and auditable • P10: Only trusted and vetted personnel are granted access to systems, applications and data repositories • P11: Personnel are granted the minimum access to systems, applications and data repositories required for their duties • P12: Multiple methods are used to identify and authenticate personnel to systems, applications and data repositories • P13: Personnel are provided with ongoing cyber security awareness training • P14: Physical access to systems, supporting infrastructure and facilities is restricted to authorised personnel • D1: Cyber security events and anomalous activities are detected, collected, correlated and analysed in a timely manner.
International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001 The ISO/IEC 27001 is an international standard on how to manage information security. It details requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS). For the purposes of the Assessment program the following sections were referenced: • 5.2 Policy • 6.1 Actions to address risks and opportunities • 6.2 Information security objectives and planning to achieve them • 7.2 Competence • 7.5 Documented information • 8.1 Operational planning and control

Control Framework
• 8.2 Information security risk assessment • 8.3 Information security risk treatment • 9.1 Monitoring, measurement, analysis and evaluation • 10.1 Nonconformity and corrective action • 10.2 Continual improvement.
ASAE3150 Assurance Engagement on Controls ASAE3150 is the Australian Auditing and Assurance Standards Board framework applied to engagements that provide an assurance report on controls at an entity. This standard will inform the procedures, practices and reporting for the assessments.

Control Measure
The COVIDSafe Application PIA[17] (dated 24 April 2020) A PIA is a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact. The PIA process was undertaken, in parallel to the development of the COVIDSafe app, to allow the DoH to consider the relevant information flows, determine whether the COVIDSafe app includes appropriate privacy obligations and protections, and if not, determine what steps should be taken to address and mitigate identified privacy risks. The privacy risks and recommendations identified through the PIA process will be evaluated as part of this assessment.
Bilateral Agreements[18] Bilateral Agreements between the DoH, acting on behalf of the Australian Government, and state and territory Health Authorities have been established to enhance contract tracing activities by states and territories to respond to, manage and control COVID-19.

[17] A PIA is not formally considered a Control Framework, however, is considered relevant to this assessment as it outlines recommendations to be implemented and access requirements.

[18] A Bilateral Agreement is not formally considered a Control Framework, however, is considered relevant to this assessment as it outlines STHA access requirements.

Control Measure
These agreements supplement the Privacy Act, relevant state and territory public health and privacy legislation and outline the arrangements for access, use and disclosure of COVIDSafe data.

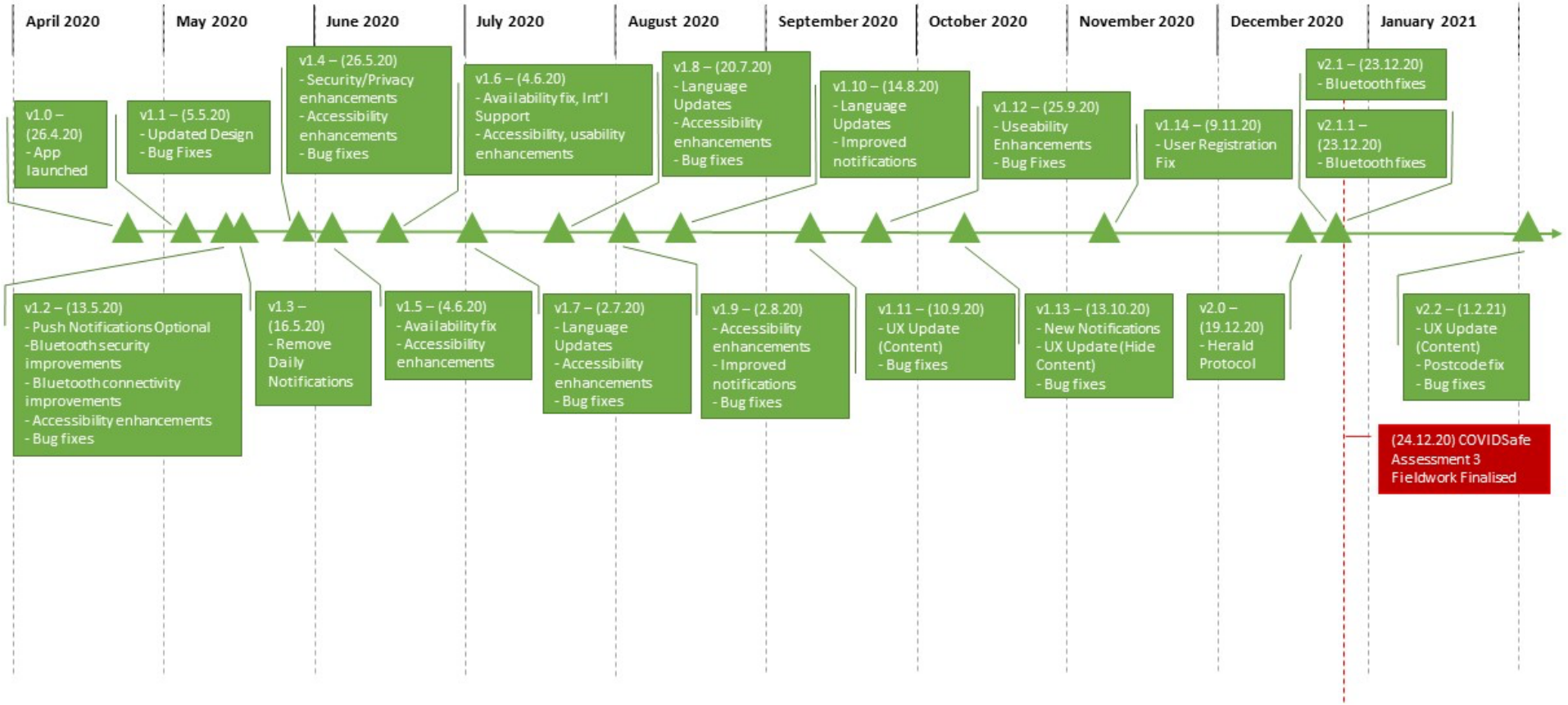
Appendix D: Privacy Risk Guidance

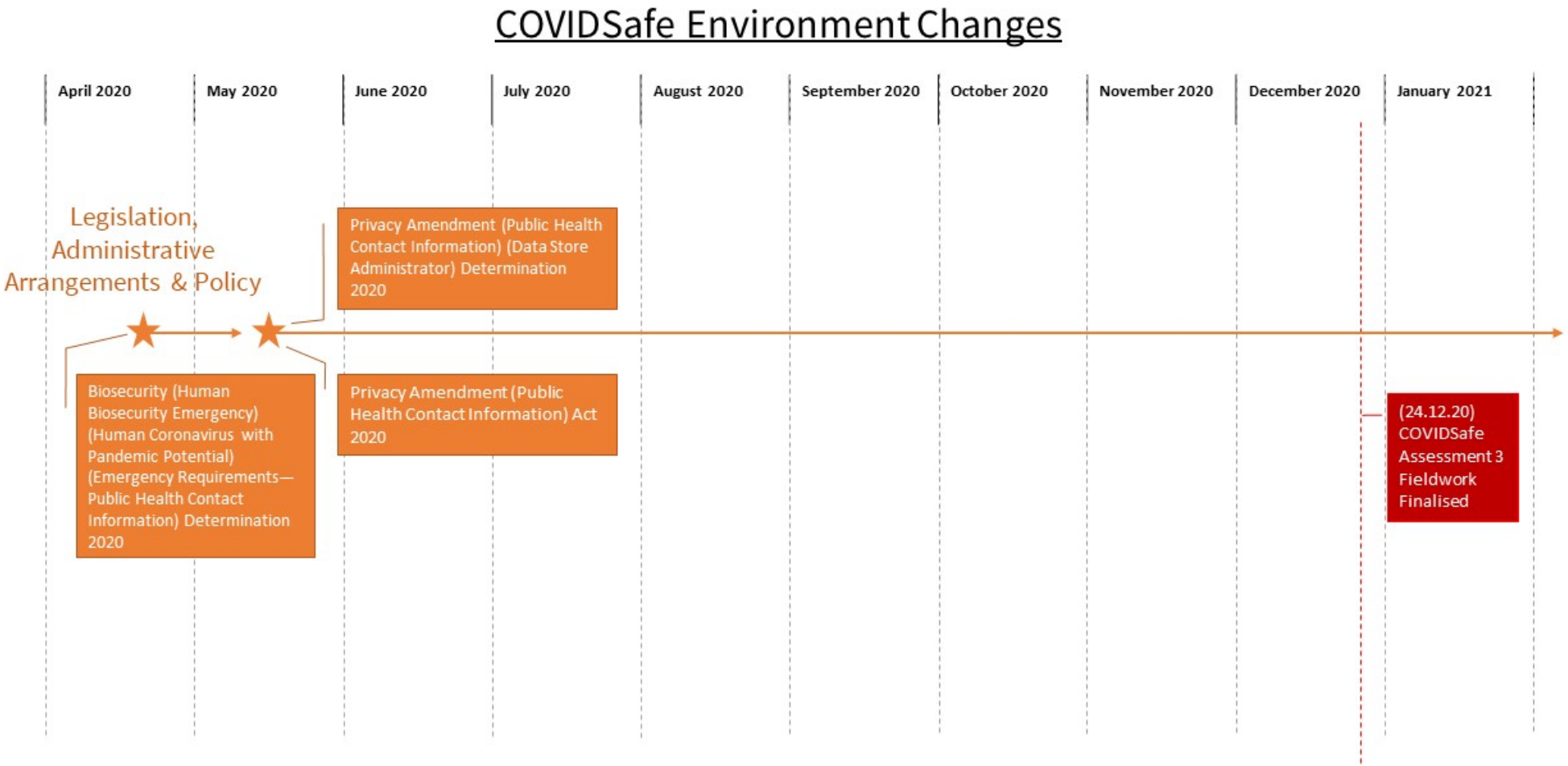
Privacy risk rating	Entity action required	Likely outcome if risk is not addressed
High risk Entity ***must***, as a high priority, take steps to address mandatory requirements of Privacy and related legislation	**Immediate management attention is required** This is an internal control or risk management issue that if not mitigated is likely to lead to the following effects	• Likely breach of relevant legislative obligations (for example, APP, TFN, Credit, privacy safeguard, Part VIIIA) or not likely to meet significant requirements of a specific obligation (for example, an enforceable undertaking) • Likely adverse or negative impact upon the handling of individuals' personal information • Likely violation of entity policies or procedures • Likely reputational damage to the entity, such as negative publicity in national or international media • Likely adverse regulatory impact, such as Commissioner Initiated Investigation (CII), enforceable undertakings, material fines • Likely ministerial involvement or censure (for agencies)
Medium risk Entity ***should***, as a medium priority, take steps to address Office expectations around requirements of Privacy and related legislation	**Timely management attention is expected** This is an internal control or risk management issue that may lead to the following effects	• Possible breach of relevant legislative obligations (for example, APP, TFN, Credit, privacy safeguard, Part VIIIA) or meets some (but not all) requirements of a specific obligation • Possible adverse or negative impact upon the handling of individuals' personal information • Possible violation of entity policies or procedures

Privacy risk rating	Entity action required	Likely outcome if risk is not addressed
		• Possible reputational damage to the entity, such as negative publicity in local or regional media • Possible adverse regulatory impacts, such as Commissioner Initiated Investigation (CII), public sanctions (CII report) or follow up assessment activities • Possible ministerial involvement or censure (for agencies)
Low risk Entity ***could***, as a lower priority than for high and medium risks, take steps to better address compliance with requirements of Privacy and related legislation	**Management attention is suggested** This is an internal control or risk management issue, the solution to which may lead to improvement in the quality and/or efficiency of the entity or process being assessed	• Risks are limited, and may be within acceptable entity risk tolerance levels • Unlikely to breach relevant legislative obligations (for example, APP, TFN, Credit, privacy safeguard, Part VIIIA) • Minimum compliance obligations are being met

Appendix E

COVIDSafe App Technical Changes




COVIDSafe Environment Changes
April 2020
May 2020
June 2020
July 2020
August 2020
September 2020
October 2020
November 2020
December 2020
January 2021
Legislation, Administrative Arrangements & Policy
Privacy Amendment (Public Health Contact Information) (Data Store Administrator) Determination 2020
Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements—Public Health Contact Information) Determination 2020
Privacy Amendment (Public Health Contact Information) Act 2020
(24.12.20) COVIDSafe Assessment 3 Fieldwork Finalised