Office of the Victorian Information Commissioner

Misuse of Department of Health information by third party employees during pandemic response

Investigation under section 8C(2)(e) of the *Privacy and Data Protection Act 2014* (Vic)

Copyright

Table of Contents

Foreword

This investigation considered the misuse of personal information by call centre staff contracted to carry out work for the Department of Health in responding to the COVID-19 pandemic.

The enormity of the challenges and pressures the pandemic posed for the Department should not be forgotten. It was responsible for guiding the public and the rest of government to respond and adapt to the rapidly changing landscape of the pandemic.

Public trust was a necessary foundation for the Department's pandemic response. Most members of the public accepted substantial restrictions on their private lives and entrusted the Department with large amounts of personal information for the greater good of curbing the spread of the virus. Asking so much of the public comes with an expectation that the information will be treated with great care.

A key aspect of the Department's pandemic response involved call centre staff engaging with members of the public by providing information on changing health directions, monitoring compliance with the directions, performing contact tracing, and booking people in for vaccinations.

The Department recognised that it did not have internal capacity to handle increased call volumes at its call centres and decided to seek more resources to do so. This was understandable.

The Department therefore outsourced some call centre operations to an external provider. In order for the contractors to do their job, they needed access to information held by the Department. However, the Department failed to take steps to ensure that all external staff who had access to that information could be trusted with it.

This investigation found that the Department did not ensure there was sufficient pre-employment screening of external staff to determine their suitability to handle personal information that had been entrusted to the Department by the public.

One of the safeguards that was put in place – the performance of police checks – was not always effective, as the Department did not submit any police check applications for processing for a period of eight months.

One of the cases of misuse of personal information covered in this investigation highlights the significant impact of these omissions.

One external staff member – who had a relevant criminal history and who was on bail at the time – used personal information from a departmental system to attend at the home of a woman who was isolating.

He pretended to be an Inspector from the Department and falsely told the woman that she was breaching her isolation requirements and could get into a lot of trouble, including being deported. He used these threats to try to coerce the woman into participating in sexual acts.

In sentencing the external staff member for committing aggravated burglary and attempting to procure sexual act by threat, the judge noted that:

> *Within this role you were privy to personal information provided by the public who were entitled to believe that in doing so, their private details would not be misused.*

The COVID 19 pandemic was a serious threat to public health. At the most acute phases, it required strong and urgent public health response. However, this investigation is a stark reminder of the harms that can stem from the misuse of personal information. The judge describing the impact on the victim as follows:

> *This offending has had a profound impact upon her, and as a consequence, she has developed Post-Traumatic Stress Disorder. She feels very insecure, so much so that she had to move away from Melbourne (her home for 9 years) to another state, where she found it difficult to find a new job. [She] is scared of being alone, she is scared of walking on the street, frequently becomes tearful, has trouble sleeping and wakes up with nightmares. She has sought psychiatric assistance for her pain and stress, which she describes as "the shadow of a lifetime".*

There will be future health emergencies that require strong and urgent government response. Those situations will bring with them obvious and significant operational pressures. Things move quickly and there are imperatives to limit the damage caused by the emergency at hand.

However, even when responding to an emergency, organisations must adequately protect personal information. Doing so requires advance planning to identify and mitigate risks of misuse of personal information. Failing to do so risks harms both to individuals and to the public's trust in government.

With this in mind, the report makes recommendations to the Department to ensure its emergency management planning includes the identification and mitigation of risks posed to information privacy associated with mobilising a surge workforce and contracting service providers.

Executive Summary

1. The Department of Health (**Department**) was allocated responsibility for leading the public health response to the COVID-19 pandemic following the split of the former Department of Health and Human Services on 1 February 2021.[1] During 2021, the Department reported that work in relation to the pandemic response greatly increased.[2]

2. Due to developments in the COVID-19 pandemic response, the Department anticipated that pandemic related activities would exceed the capacity of the Department's existing call centres. As a result, the Department identified and engaged business process outsourcing (**BPO**) vendors to assist to meet the high demands of the public directions hotline. One of the BPOs engaged was Acquire BPO Australia Pty Ltd (**Acquire**).

The breaches

3. During 2021, two separate instances of information misuse involving Department-held personal information occurred. The incidents were unrelated, however both incidents involved staff working at Acquire call centres. They will be referred to in this report as **Breach 1** and **Breach 2**.

4. **Breach 1** involved Subject 1, a casual employee at Acquire who was employed to undertake departmental work for the COVID-19 response. Subject 1 used personal information accessed through the course of his employment to attend the home of a woman (the victim) and posed as an authorised officer. Subject 1 was not an authorised officer and his attendance at the woman's home was not in connection with his duties at Acquire. While at the victim's home, Subject 1 attempted to pressure the victim into performing sexual acts by incorrectly telling her she was 'not complying with the isolation requirements and she could get in a lot of trouble'.[3]

5. Since then, the victim has suffered post-traumatic stress disorder, has had to relocate interstate, and feels unsafe when on her own.[4]

6. **Breach 2** involved Subject 2, a casual employee at Acquire also undertaking departmental work for the COVID-19 response. Subject 2 was arrested on 31 August 2021, on multiple criminal charges including armed robbery. After the arrest, Victoria Police officers seized and searched Subject 2's mobile phone.[5]

---

1 Department of Health, Annual Report 2020-21, available at: https://www.health.vic.gov.au/sites/default/files/2021-10/department-health-annual-report-2020-21.pdf, accessed on 7 March 2023.
2 Department of Health, Annual Report 2020-21,, available at: https://www.health.vic.gov.au/sites/default/files/2021-10/department-health-annual-report-2020-21.pdf, accessed on 7 March 2023.
3 County Court, DPP v Awow [2022] VCC 1353, available at; sentencing-remarks-dpp-v-awow.pdf (countycourt.vic.gov.au)
4 County Court, DPP v Awow [2022] VCC 1353, available at; sentencing-remarks-dpp-v-awow.pdf (countycourt.vic.gov.au)
5 Information Provided to OVIC by Victoria Police

7. The search of Subject 2's mobile phone found a photo of a computer screen showing an information system that contained an address. The embedded metadata in the image indicated that the photo was taken in the vicinity of Subject 2's workplace. The photo was taken on 25 July 2021, three days after Subject 2's employment began at Acquire.[6]

8. The photo on Subject 2's phone was of a screen from a departmental data management system that this investigation shows is likely the COVID-19 Vaccination Management System (**CVMS**).

9. The investigation did not identify any evidence that suggests Subject 2 used this information for criminal activity.

The investigation and findings

10. Under section 8C(2)(e) of the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**), the Privacy and Data Protection Deputy Commissioner (**Deputy Commissioner**) can undertake an investigation to decide whether to issue a compliance notice. Under section 78 of the PDP Act, the Deputy Commissioner may serve a compliance notice on an organisation if satisfied that serious, flagrant, or repeated breaches of the Information Privacy Principles (**IPPs**) have occurred. A compliance notice requires an organisation to take specified action within a specified period for the purpose of ensuring compliance with the IPPs.

11. On 19 November 2021 the Deputy Commissioner decided to commence this investigation.

12. OVIC's investigation considered whether the Department took reasonable steps to protect personal information it holds from misuse, as required by IPP 4.1.

13. The findings of the investigation relate to three main themes:

- recruitment and pre-employment screening steps for contracted staff at Acquire;
- responsibility and management of the Department's engagement with Acquire, including employee screening; and
- data management systems and training used by staff at Acquire.

Theme 1 – recruitment and pre-employment screening

14. When the Department engaged Acquire on 1 January 2021, Acquire began recruiting staff rapidly. The application process was informal, and successful candidates commenced training and work within days of first being contacted.

15. The Deputy Commissioner found that there was insufficient pre-employment screening of these call centre staff. That is, the Department did not sufficiently plan for or mitigate risks that

[6] Information Provided to OVIC by Victoria Police

unsuitable or ineligible staff sourced from external providers would be given access to personal information and would then misuse it. She found that this was a contravention of IPP 4.1.

16. Staff were told that they would be required to complete a police check and sign a statutory declaration declaring that they did not have any criminal history. It was intended that staff would begin work while the police check applications were being processed.

17. Both Subject 1 and Subject 2 provided completed police check applications when they began work at Acquire. However, across a period of eight months from the commencement of the engagement with Acquire, the Department did not submit police check applications for processing for any Acquire staff.

18. This meant that no police check application was ever submitted in relation to Subject 1 while the submission of Subject 2's police check application was delayed by three weeks.

19. As a result, neither Acquire nor the Department was aware of Subject 1's criminal history. A police check of Subject 1 would have revealed a prior criminal history, including that Subject 1 was on bail at the time of his employment. This would have precluded him from being employed by Acquire to undertake departmental work – and from carrying out the criminal conduct which eventuated.

20. The Deputy Commissioner found that the Department contravened IPP 4.1 by failing to expediently submit police check applications for Acquire call centre staff.

Theme 2 – responsibility and management of the Department's engagement with Acquire, including employee screening

21. The initial engagement of Acquire by the Department was informal and the initial process of assigning responsibility for submitting police check applications was also informal.

22. The Department and Acquire then executed a formal services agreement in February 2021 which included a clause setting out responsibility for pre-employment screening.

23. The clause required that, at the request of the Department, Acquire would be responsible for conducting pre-employment probity checks including police checks. From the commencement of the engagement with Acquire, however, the Department told Acquire that the Department would have responsibility for submitting police check applications to be processed.

24. There was confusion and inconsistency within the Department about which party was, in fact, responsible for submitting police check applications.

25. The Department reviewed the process for submitting police check applications after becoming aware of Breach 1. This revealed that, for a period of around eight months, police check applications were being forwarded to the Department by Acquire but were not being submitted by the Department for processing.

26. The services agreement was extended twice during 2021 before Breaches 1 and 2 occurred. These extension processes provided opportunity for the Department to review the contract and parties' adherence to their respective obligations, including pre-employment screening steps. However, the issue of the non-submission of police check applications was not detected.

27. The Deputy Commissioner found the Department did not clearly and unambiguously define respective roles and obligations for the submission of police check applications in its contractual arrangements with Acquire. Additionally, the Department did not systemically review whether contractual obligations relating to police checks were being met before Breach 1 occurred. She therefore found that the Department contravened IPP 4.1.

Theme 3 – data management systems and training

28. The Department's data management systems had a range of security measures in place, including individual user login credentials, system logs and multi-factor authentication (MFA).

29. The MFA method in place required all users of relevant departmental systems to use their mobile phone to verify their identity. This included Agents conducting departmental work and who therefore needed to have their phone with them while working.

30. This reduced the effectiveness of Acquire's ability to enforce a no-phone policy. However, the Department reported that there were no alternative methods of MFA that were feasible in the circumstances.

31. The Deputy Commissioner found that the Department did not contravene IPP 4.1 in relation to the method of MFA it implemented. It was appropriate for the Department to implement MFA. It may have been preferable to use a method that did not require the use of a mobile phone but, once the pandemic response had begun, this was not a reasonably practicable step to implement.

32. The Deputy Commissioner found that the training provided to Acquire Agents regarding appropriate handling of personal information was minimal due to the urgent need to commence taking calls as part of their work for the Department.

33. The Deputy Commissioner found, however, that the Department did not contravene IPP 4.1 in terms of the training provided to Acquire Agents. That is because it would have been abundantly obvious to Subjects 1 and 2 (and to other Agents) – who signed Confidentiality Undertakings – that misusing personal information in the manner they did was clearly inappropriate and unauthorised. It is unlikely that additional training would have prevented the misuse of personal information that eventuated.

Recommendations

34. The Deputy Commissioner determined that the Department's contraventions of IPP 4.1 were serious for the purposes of s 78(1)(b)(i) of the PDP Act.

35. However, the Deputy Commissioner determined that it would be inappropriate and ineffective to issue a compliance notice – which requires that an organisation take 'specified action'.

36. The investigation identified issues that are necessarily broad rather than specific in nature. As such, the Deputy Commissioner has instead issued the Department with recommendations. This intentionally places responsibility on the Department to determine the specific actions required to address the issues identified by the Deputy Commissioner.

37. The Deputy Commissioner recommended that the Department reviews its emergency management planning policies and procedures to ensure they adequately address the following:

    1. Preparedness for the recruitment of surge workforces which adequately considers and mitigates associated privacy risks including:

        a. the risk of ineligible or unsuitable externally contracted staff gaining access to personal information held by the Department (this may include, for example, contingency planning for expedited police checks and the development of minimum recruitment and character standards to be adhered to by contracted service providers); and

        b. the need to review the appropriateness of access controls to Department systems for externally contracted staff.

    2. Assignment of responsibility to a senior department employee (reporting directly to the Secretary) to ensure that for contracts executed with contracted service providers associated with emergency management response:

        a. Contract creation – responsibility for obligations relating to the protection of personal information is clearly and appropriately assigned between the Department and the contracted service provider; and

        b. Contract management – adherence by both parties to obligations relating to the protection of personal information is systematically reviewed and verified.

Procedural fairness and privacy

38. OVIC gives regulated bodies a reasonable opportunity to respond to potentially adverse findings. OVIC takes into account any response from a regulated body before finalising and issuing an investigation report.[7]

39. This report contains adverse comments and opinions about the Department. In accordance with the Deputy Commissioner's obligations to afford the Department natural justice, the

[7] OVIC, Regulatory Action Policy 2022.

Department was given a reasonable opportunity to respond to the adverse material, and this report includes the Department's response to the report (see Annexure A).

40. Whilst Acquire is not subject to adverse findings in the report, it was nevertheless given a reasonable opportunity to respond to relevant material in the report. Acquire provided submissions before the finalisation of the report but did not provide a response to be published with the report.

41. Whilst the report does not specifically name individuals, it includes information that may identify persons, such as individuals employed by the Department at the relevant time and who had relevant expertise or knowledge of events. These individuals were not the subject of the investigation and are therefore not the subject of adverse findings in the report.

Part 1 – Introduction

Background

COVID-19 pandemic development

42. On 16 March 2020, the Victorian Government declared a State of Emergency in response to the COVID-19 pandemic. The Government introduced various measures to ''flatten the curve' of COVID-19 and give [Victoria's] health system the best chance of managing its response to the virus.'[8]

43. The Department of Health and Human Services was the Victorian government agency that was responsible for the state's health system and public health social policy.[9] The measures introduced by the State of Emergency required substantial operational changes at the Department of Health and Human Services.

44. On 30 November 2020 it was announced that the Department of Health and Human Services would be separated into two new Departments - the Department of Health and the Department of Families, Fairness and Housing.[10]

45. The Department of Health (**Department**), was formally established on 1 February 2021 which sought to deliver a health system that focused on improving patient outcomes and experience for all Victorians.[11] The divisions and work units involved in the COVID-19 response, including contact tracing and vaccination bookings, became part of the Department of Health. The breaches that are the subject of this investigation occurred after the establishment of the Department of Health. As such, the Department of Health is the department under investigation.

46. The Department was designated as the control agency in charge of the COVID-19 emergency response. This role required the establishment of new systems and processes; changes to existing departmental processes; and ongoing management of these systems and processes.

47. Shortly after the State of Emergency was declared, the Chief Health Officer (**CHO**) authorised Officers to exercise significant powers under the *Public Health and Wellbeing Act 2008* to eliminate or reduce a serious risk to public health, including by detaining people, restricting

---

8 https://www.premier.vic.gov.au/state-emergency-declared-victoria-over-covid-19
9 https://www.health.vic.gov.au/about
10 Department of Health, Annual Report 2020-21, available at: https://www.health.vic.gov.au/sites/default/files/2021-10/department-health-annual-report-2020-21.pdf, accessed on 7 March 2023.
11 Department of Health, Annual Report 2020-21, , available at: https://www.health.vic.gov.au/sites/default/files/2021-10/department-health-annual-report-2020-21.pdf, accessed on 7 March 2023.

movement, preventing entry to premises, or providing any other direction the Authorised Officer considered reasonable to protect public health. [12]

48. On 30 December 2020, Victorian authorities identified three community cases of COVID-19, ending 61 days of Victoria reporting zero cases. As a result of this, the border with New South Wales was closed and a mandated 14-day isolation period was introduced for all returning travellers arriving after 11:59pm 31 December 2020.[13]

> *On 30 December 2020, with border closures in place between NSW and Victoria and unprecedented volume of requests for assistance to the Public Directions hotline, it became apparent that the Department's existing business process outsourcing vendors, [named companies] would not be able to adequately meet the resource demands required to maintain this service. At this time, calls to the hotline exceeded forecasts for this period by at least 100 per cent.'*[14]

49. Due to rapid developments in the COVID-19 pandemic, the Department of Health's call centres were under significant pressure to undertake pandemic related activities. As a result, the Department identified an urgent need to increase the capacity of its COVID-19 call centres to assist in the management of these responsibilities.

Engagement of external call centre companies

50. On 1 January 2021, the Department engaged Acquire BPO Australia Pty Ltd (**Acquire**) to assist it to manage the overflow of call-centre work caused by changes to COVID-19 restrictions. Acquire is a private company that specialises in providing outsourced back-office support, customer acquisition, customer service, technical support, and software development.[15]

51. The Department engaged a total of five external providers to support call centre operations required during the pandemic. Acquire was one of two BPOs engaged in early January 2021. Acquire commenced providing services on 2 January 2021, one day after it was contacted by the Department.[16]

52. The Department followed a procurement process for the engagement of Acquire, informed by the Department's Critical Incident Procurement Policy (**CIPP**).[17] The CIPP provides a process for

---

[12] Section 3 of the *Public Health and Wellbeing Act 2008* defines an Authorised Officer. Section 165AW of the *Public Health and Wellbeing Act 2008* states that the Chief Health Officer my authorise authorised officers to exercise any of the public health risk powers and pandemic management powers for the purpose of eliminating or reducing serious risk to public health.

[13] https://www.dhhs.vic.gov.au/coronavirus-update-victoria-31-december-2020

[14] Former Department Director of Contact Centre Operations Affidavit, 4 November 2022

[15] https://acquirebpo.com/

[16] Review Report provided by Department

[17] Correspondence from Department to OVIC

procurement activities 'where full compliance with standard VGPB[18] procurement policies would seriously delay the Department's ability to immediately respond to an emergency, crisis or disaster'.[19]

53. A services agreement between the Department and Acquire was negotiated in the weeks that followed and was finalised on 16 February 2021.

54. The requirements schedule which accompanied the services agreement between the Department and Acquire, outlines the services to be provided by Acquire. This included:

- providing information and support to the Victorian community on latest COVID directions and restrictions;
- contact and case outbreak management;
- quarantine check-in calls; and
- COVID vaccination program.[20]

55. While this arrangement was in force, two instances of personal information misuse were identified as having occurred involving staff working at Acquire call centres. These incidents are the subject of this investigation and are referred to as Breach 1 and Breach 2 in this report. OVIC is not aware of any other breaches occurring in these circumstances.

What systems did contracted staff have access to and what information did they hold?

56. Contracted staff working for BPOs engaged by the Department had access to three main departmental information systems necessary to complete their work.

- COVID-19 Vaccination Management System (CVMS)
    i. a COVID-19 vaccination booking system used by the vaccination general inquiry line to make and amend vaccination bookings.
- Genesys
    i. an integrated telephony, call recording and desktop information system used by Agents to make and receive calls to and from the public as part of the COVID-19 response.
- Secondary Close Contact (SCC) application

[18] Victorian Government Purchasing Board
[19] Critical Incident Procurement Policy
[20] Requirement Schedule between Department and Acquire

i. a program used to upload secondary close contact information into a central data depository known as the Transmission, Results, Epidemiology Victoria Information System (TREVI). The SCC application was a data depository form, meaning Agents did not have access to information once it has been submitted. This application has been decommissioned.

CVMS
Accessed on a web browser with unique CVMS email username and the Agent's password. The Agent is then required to provide two-factor authentication through the Microsoft Authenticator Application or via SMS on their mobile phone to gain access.

Genesys
Accessed on a web browser using a Single Sign On (SSO) via Microsoft Authenticator Application on their mobile phone.

Secondary Close Contact
The same authentication process as Genesys through the SSO.

57. The first two of these systems – the CVMS and Genesys were most relevant to the investigation.

What is the COVID-19 Vaccination Management System and how was it used?

58. In early 2021, the Department developed CVMS.[21] The system was developed to assist the Department to perform its functions related to the COVID-19 pandemic response. The tasks performed by Agents on CVMS were the confirmation and cancellation of vaccination bookings.

59. CVMS can be accessed and used in three main ways.

- public portal – accessible by members of the public to book vaccination appointments.
- clinician portal – accessible by health professionals to record information about vaccines administered.

[21] Interview with Department IT Employees

- **Command centre interface** – accessible by departmental employees and contractors, to enter information, manually book vaccination appointments and, depending on the type of access, run and extract reports.

60. Agents of BPOs answering the Coronavirus Hotline had 'command centre interface' access.[22] Within this level, Agents were assigned to a security group that only allowed them to access the Contact Centre Application. The Department reported that Agents would be unable to access the auditing features of the command centre interface and as such would have been unable to extract data.[23] OVIC investigators confirmed during a system demonstration that Agents were able to freely search for individuals on CVMS.[24]

61. The information contained in CVMS was accessible to the Agents to enable them to perform the designated task of updating vaccination bookings. The Department reported the following personal information was visible to Agents on CVMS:

- Surname, first name, date of birth, address, mobile number, home number, email address, ethnicity, COVID-19 immunisation history, upcoming COVID-19 vaccination appointments, next of kin details of individuals that booked a COVID-19 vaccination.[25]

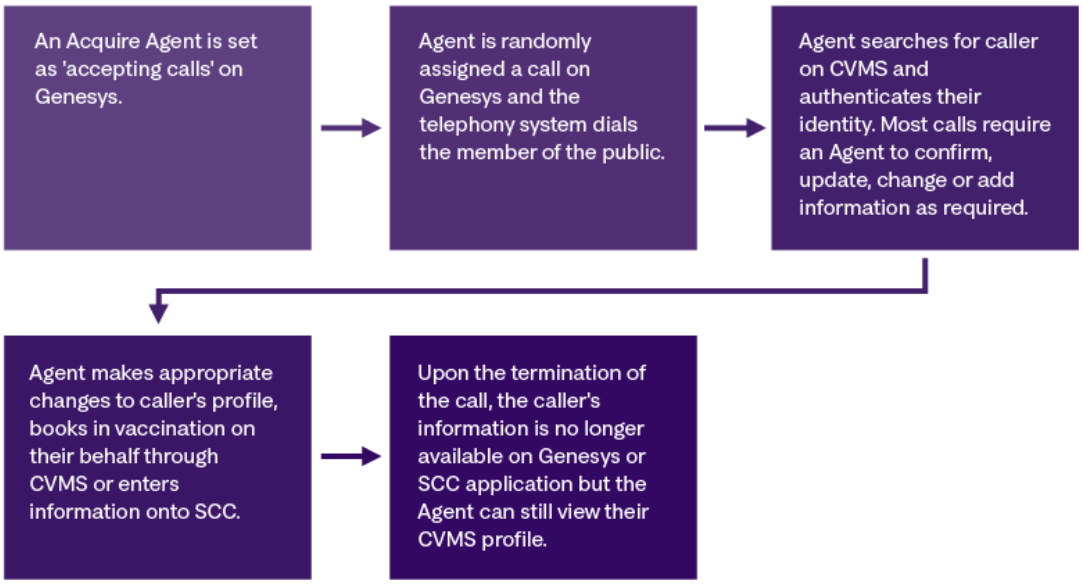
What is Genesys and how was it used?

62. Genesys is an integrated telephony system used to make and receive calls from a desktop. The system pushes individual records (a Case) in a queue to the desktop of the agent who will then take the call. The Agent is only able to access a case when they are working on it and are unable to preview cases in their queue or revisit cases which have been completed.

63. The cases held personal and health information of citizens which was used to support conversations around contact tracing and vaccinations, including the confirmation and updating of such information.[26]

[22] Interview with Department IT Employees
[23] Interview with Department IT Employees
[24] Systems demonstration given to OVIC investigators
[25] Correspondence from Department to OVIC
[26] Correspondence from Department to OVIC

64. The Department informed OVIC that the process of an Agent *making an outbound call* to a member of the public was reported to OVIC as follows[27]:



65. The Department reported the following personal information is visible to Agents on Genesys:

- Surname, first name, sex, date of birth, address, mobile number, home number, email address, Aboriginal or Torres Strait Islander status, language spoken at home or if an interpreter is required, parent/guardian, exposure site, TREVI case number (separate system), CMM ID (separate system), PHESS ID (separate system). [28]

Breach 1

66. On 31 May 2021, an individual (**Subject 1**) began working for Acquire. On his first day he was asked to bring documentation and information for onboarding purposes. Subject 1 brought his payment details, superannuation information, and identity verification documents required to undertake a police check.

67. At this point in time, although Agents completed the paperwork needed for a police check when starting their job, they began work before the checks were processed due to the Department's need to have Agents taking calls as soon as possible.

68. Because of this arrangement, the Department and Acquire implemented a system whereby employees would sign a statutory declaration declaring that they did not have any criminal

[27] Interview with Department IT Employees
[28] Correspondence from Department to OVIC

convictions, pending criminal charges, employment disciplinary actions or findings of improper or unprofessional conduct. Employees also signed a Confidentiality Undertaking.

69. Subject 1 signed a statutory declaration on his first day declaring he did not have any charges or convictions and a Confidentiality Undertaking asserting that he would not disclose departmental information to outside sources. He also completed a police check application form, but the police check application was not submitted for processing by the Department.

70. Acquire uploaded all completed police check forms to a DropBox created by the Department for this purpose. Subject 1's police check was never submitted for processing. Had it been submitted the police check would have revealed prior criminal history, including using a carriage service to menace and unauthorised use of information.

71. Subject 1 was provided with login credentials following limited training that allowed him access to departmental information systems necessary for him to do his job in the COVID-19 response call centre. These included the CVMS and the Genesys telephony systems. Subject 1 then had access to personal information of Victorians and others as part of his role of making and receiving calls on behalf of the Department's COVID-19 response.

72. Subject 1 continued to have access to the Department's systems for over 59 days.

73. On 14 July 2021, Subject 1 called the victim, who had returned to Victoria from New South Wales four days prior and was isolating in accordance with health orders. The call was made as part of Subject 1's role at the call centre.

74. At the conclusion of the call, Subject 1 took a photo of his computer screen which contained the victim's personal information. Following the conclusion of his shift, Subject 1 called the victim again from their own mobile phone. Subject 1 impersonated an Authorised Officer and told the victim that he would be conducting a home inspection within the next half an hour.

75. Subject 1 then went to the victim's home, where they were isolating. At approximately 9pm on 14 July 2021, Subject 1 telephoned the victim from outside her home.

76. On the belief that Subject 1 was an Authorised Officer, the victim allowed him into their residence. Subject 1 then told the victim, who was an international student, that they had failed to meet the Government's requirements of home isolation, and implied that they might be deported as a result. Subject 1 then sought to pressure the victim into sexual acts and the victim refused. After continually requesting sexual acts, Subject 1 was told to leave the house by the victim.

77. Subject 1 called the victim five times after leaving the house.

78. The victim reported the incident to Victoria Police shortly after Subject 1 left the residence.

79. Victoria Police notified the Department of a criminal investigation into the activities of an unidentified employee of Acquire on 3 August 2021.

80. On 4 August 2021, Subject 1's employment with Acquire was terminated due to their failure to attend work.[29]

81. On 6 August 2021, Victoria Police identified Subject 1 to the Department and Acquire and his access to all systems was revoked on the same day.[30]

82. Subject 1 was prosecuted and convicted for the actions he carried out on 14 July 2021. The sentencing remarks related to Subject 1's trial indicates that this offence has had a 'profound impact' on the victim.[31] The victim has had to move states and suffers from Post-Traumatic Stress Disorder due to Subject 1's offending.

83. Subject 1 pleaded guilty to two offences involving his actions on 14 July 2021. These were:

- one charge of aggravated burglary, contrary to s 77(1) of the Crimes Act 1958; and
- one charge of attempted procuring sexual act by threat, contrary to ss 321M and 44(1) of the Crimes Act 1958.

84. He was sentenced on 23 August 2022.

85. The seriousness of the offences and the role the information misuse had in the matter are outlined by her Honour Judge Ellis. She wrote in Subject 1's sentencing remarks that he had been 'privy to personal information provided by the public who were entitled to believe that in doing so, their private details would not be misused'.

Breach 2

86. On 23 July 2021, a different person began working at Acquire (**Subject 2**)[32]. In a welcome email, they were told to bring 100 points of ID on their first day and that they would 'be required to complete a police check consent form on the day'.

87. As with Subject 1, although Agents completed the paperwork needed for a police check when starting their job, Subject 2 began work before it was processed. This was in accordance with the procedures established between the Department and Acquire.

88. Subject 2 signed a statutory declaration on their first day declaring they did not have any criminal history and a Confidentiality Undertaking declaring that they would not disclose departmental information to outside sources. They also completed a police check application

[29] Correspondence from Acquire to OVIC
[30] Correspondence from Department to OVIC
[31] County Court, DPP v Awow [2022] VCC 1353, available at; sentencing-remarks-dpp-v-awow.pdf (countycourt.vic.gov.au)
[32] Correspondence from Department to OVIC; Correspondence from Acquire to OVIC

form, but although Acquire sent this to the Department for processing, the police check application was not submitted for processing by the Department.

89. The Department reviewed the process for submitting police checks after becoming aware of Breach 1 and the fact that no police check application had been submitted for Subject 1. This review revealed that, for a period of around eight months, police check applications were being forwarded to the Department by Acquire but were not being submitted by the Department to be processed.

90. It was at this point, more than three weeks after Subject 2 began their employment, that it was identified that no police check application had been submitted for Subject 2. Acquire directly submitted the police check application for Subject 2 on Wednesday 18 August 2021, after the processing issue had been identified and the Department had directed all BPOs to process police checks on Friday 13 August 2021.

91. Acquire ended Subject 2's casual employment on 26 August 2021 due to their failure to attend work.[33]

92. On 31 August 2021, Victoria Police arrested Subject 2 on multiple criminal charges including armed robbery. After the arrest, Victoria Police officers seized and searched Subject 2's mobile phone.[34]

93. The search of Subject 2's mobile phone found a photo of a computer screen showing an information system that contained an address. The embedded metadata in the image indicated that the photo was taken in the vicinity of Subject 2's workplace. Subject 2 later confirmed to police that the photo was taken at their workplace.[35] The photo was taken on 25 July 2021, three days after Subject 2's employment began at Acquire.[36]

94. The photo on Subject 2's phone was of a screen from a departmental data management system called the CVMS (**Breach 2**). The information on the screen included a street number, street name, and a suburb.[37]

95. Subject 2 did not have a criminal history during the time they were employed at Acquire. The outcome of Subject 2's police check was returned on 22 September 2021, by which date they had two pending charges dated after their employment at Acquire had ceased.[38]

96. OVIC is not aware of any evidence that suggests Subject 2 used this information for criminal activity.

---

[33] Department Review Report
[34] Information Provided to OVIC by Victoria Police
[35] Information Provided to OVIC by Victoria Police
[36] Information Provided to OVIC by Victoria Police
[37] Image provided to OVIC by Victoria Police
[38] Returned Police Check outcome for Subject 2

Conduct of investigation

Reasons for undertaking the investigation

97. The Privacy and Data Protection Deputy Commissioner first became aware of Breach 1 on 13 August 2021, when a Member of Parliament wrote to OVIC. The member expressed concern following media reporting of an incident involving the misuse of government information. Media reporting indicated that the person alleged to have used this information 'was hired by a company contracted to complete research and data analysis for the Department of Health's COVID contact tracing team'.[39] This report related to Breach 1.

98. Due to the serious nature of the breach, OVIC commenced preliminary inquiries with the Department of Health in line with its Regulatory Action Policy.

99. On 9 September 2021, the Department contacted OVIC to notify it of Breach 2.

100. The Deputy Commissioner considered both the real and potential consequences of this misuse of information by Subject 1 and Subject 2, and the fact that both Subjects were working for the same BPO. The Deputy Commissioner considered the commonalities between the two could present a serious risk to the people whose information was stored and collected during the COVID-19 pandemic, and that the misuse might point to a serious contravention of the IPPs by the Department. The Deputy Commissioner decided to commence an investigation under sections 8C(2)(e) and 78 of the PDP Act.[40]

101. Under section 8C(2)(e) of the PDP Act, the Deputy Commissioner can undertake an investigation to decide whether to issue a compliance notice. Under section 78 of the PDP Act, the Deputy Commissioner may serve a compliance notice on an organisation if satisfied that serious, flagrant, or repeated breaches of the IPPs has occurred. A compliance notice requires an organisation to take specified action within a specified period for the purpose of ensuring compliance with the IPPs.

Information Privacy Principle 4.1

102. Part 3 of the PDP Act requires Victorian public sector organisations[41] to handle personal information in accordance with 10 Information Privacy Principles (**IPPs**) found in Schedule 1 of

[39] The ABC, Victoria Police allege man impersonated COVID-19 inspector and demanded sex from woman - ABC News

[40] Correspondence from Department to OVIC

[41] Section 13 sets out those entities considered public sector organisations that are bound to comply with the IPPs. It includes public sector agencies (such as Departments), local councils and Victoria Police. It also includes some private entities – contracted service providers – but only where they are providing services under a State contract and the contract contains a clause specifying that the CSP will be directly bound by the IPPs.

the PDP Act. Section 20 of the PDP Act states that an organisation must not do an act, or engage in a practice, that contravenes an IPP.

103. IPP 4 relates to information security. IPP 4.1 states:

> An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

104. Personal information is defined in section 3 of the PDP Act, in summary, as information or an opinion about an individual whose identity is apparent or can be reasonably ascertained.

Scope of the investigation

105. The Deputy Commissioner's investigation considered whether the Department had contravened IPP 4.1.

106. Acquire, in relation to its provision of services associated with the COVID-19 pandemic response, is also an 'organisation' for the purpose of Part 3 (Information Privacy) of the PDP Act, because it delivers those services in accordance with a state contract containing a provision of the kind referred to in section 17(2) of the PDP Act. [42] While Acquire was also bound to comply with the IPPs in the circumstances, it was not the subject of the investigation.

107. The Deputy Commissioner's investigation sought to understand the circumstances of the breaches. The investigation sought to establish:

- the circumstances in which the two individuals were able to access and misuse personal information held by the Department;
- whether those circumstances indicate a failure by the Department to take reasonable steps to secure the personal information, as required by IPP 4.1.
- whether that contravention of IPP 4.1 was serious or repeated, and if a compliance notice should be issued.

How the investigation was conducted

108. The Privacy and Data Protection Deputy Commissioner commenced the investigation on 19 November 2021.

109. The Deputy Commissioner considered a range of information obtained during the investigation to reach the views outlined in this report including:

---

[42] Clause 7.6 of the service agreement between the Department and Acquire also states: 'The Contractor acknowledges and agrees that it is a 'contracted service provider' within the meaning of the *Privacy and Data Protection Act 2014* (Vic)'

- written submissions from the Department;
- evidence provided on affidavit from a prior departmental employee, who at the relevant time was the department's Director of Contact Centre Operations;
- information provided in examinations with three Acquire employees: Operations Manager, Chief Commercial Officer, and a personnel Manager;
- information provided in voluntary interviews with three current Department employees: Principal ICT Procurement Advisor, Director of People Services and Culture, Vendor and Contract Manager;
- information provided in one examination with a former Department employee, Manager Contact Centre Performance;
- demonstration of CVMS and Genesys by Department employees and a group interview with system administrators; and
- reviewing documentary evidence, including:
    i. internal policies of the Department and Acquire - relating to training, onboarding, and management of new employees;
    ii. correspondence between staff of the Department and Acquire;
    iii. services agreements between the Department and five BPOs, including Acquire; and
    iv. documents and information provided by Victoria Police in relation to the investigations of Subject 1's and Subject 2's actions.

110. The Deputy Commissioner thanks the Department and Acquire for their assistance in the investigation. The Deputy Commissioner notes that both the Department and Acquire have taken steps independently of this investigation to review these incidents and implement strategies to reduce the risk of similar incidents occurring again.

Part 2 – Discussion of findings

How OVIC assessed compliance with IPP 4.1

111. IPP 4.1 requires that an organisation take reasonable steps to protect personal information they hold from misuse, loss and unauthorised access, modification and disclosure.

112. Determining what security measures are 'reasonable' for an organisation to implement will depend on a number of circumstances, including:

- the impact of a potential security breach on the person the information relates to
- the nature of the organisation and difficulties implementing the step
- the likelihood of a security breach occurring
- the invasiveness of the security measure.[43]

113. Both Breaches 1 and 2 involved information misuse, as access to the information held on Departmental systems was permitted due to Subject 1's and 2's employment at Acquire. The misuse occurred when on two separate and unrelated occasions, Subject 1 and Subject 2 each took a photo with their mobile phones of personal information held on departmental systems – for reasons unrelated to work being carried out on behalf of the Department.

114. The following three chapters discuss the factors that contributed to the occurrence of the two breaches; findings made by the Deputy Commissioner; and an assessment of whether the department failed to take reasonable steps to protect personal information they hold from misuse, loss and unauthorised access, modification and disclosure in breach of IPP 4.1.

115. The factors discussed fall into three broad themes:

- recruitment and pre-employment screening undertaken for Agents engaged in departmental work;
- responsibility and management of pre-employment screening between Acquire and the Department; and
- data management systems, controls, and training.

[43] OVIC IPP Guidelines, IPP 4 – Data Security, p 4-7.

Theme 1 - Recruitment and pre-employment screening

Key points:

- When the Department engaged Acquire on 1 January 2021, Acquire began recruiting staff rapidly. The application process was informal and successful candidates would commence training and work within days of first being contacted.
- Staff were told that they would be required to complete a police check as part of the onboarding process. It was intended that staff would begin work while the police check applications were being processed.
- Both Subject 1 and Subject 2 provided completed police check applications when they began work at Acquire. In accordance with established procedures for this work, Acquire sent the police check applications to the Department for processing. However, the Department did not submit the applications for processing.
- As a result, neither Acquire nor the Department was aware of Subject 1's criminal history. A police check of Subject 1 would have revealed a prior criminal history, including that Subject 1 was on bail at the time of his employment. This would have precluded him from being employed by Acquire to undertake departmental work – and from carrying out the criminal conduct which eventuated.

Background

116. Throughout the COVID-19 pandemic the Department of Health was under substantial pressure regarding its functions related to contact tracing and public information relating to health directions issued by the CHO – such as those relating to the Border Crossing Scheme, Home Quarantine Scheme or the vaccination program.

117. In July 2020, the Department identified that 'each stage of the contact tracing process had and would continue to come under continual resourcing pressure to capture and manage the increasing case numbers in Victoria.'[44]

118. With regard to call centres, the volume of calls from the public and the resources required to manage these was largely dependent on the circumstances of the pandemic and the nature of the CHO directions in place.

[44] Correspondence from Department to OVIC

119. As a result, the Department identified potential BPO vendors to assist to meet the high demands of the public directions hotline.

120. Following an increase of COVID-19 cases in New South Wales, the CHO issued directions for a cross-border permit scheme on 18 December 2020. These directions were revoked and reissued with changes a number of times in late December 2020 and early January 2021. This included the closing of Victoria's border with New South Wales on 1 January 2021. The Department states that the cross-border permit scheme quickly led to unprecedented call volumes.

121. It was not until 1 January 2021, that the Department contacted Acquire to manage the increased call traffic to the centres.

122. On that day, a senior officer of the Department contacted an Acquire executive to ask if it was possible to get 'some Agents – approximately around a hundred on board… that day or ASAP to help with the emergency COVID demand queries'.[45]

123. According to an email chain between Department staff on 1 January 2021, Acquire had quickly identified potential Agents, some of whom commenced training the next day.[46]

How were Agents recruited?

124. The influx of calls to call centres put pressure on BPOs contracted to the Department to assist in the COVID-19 response to fill roles quickly to meet demand. BPOs filled these roles in a variety of ways including referral programs and online recruitment via social media. According to a former Department employee who was responsible for managing the performance of call centres at the time of the breaches:

> *So if we were going through a surge period, so a new outbreak or if there's new orders been put in place to lock down, we may go from requiring 100 FTEs, to 500 FTEs which is the reason why we had multiple providers, we'd be able to spread that risk across.*[47]

125. Acquire used a referral program where existing staff could refer their friends and family to increase staff quickly during surge periods. In this context a surge period refers to higher than usual operational needs during periods of a COVID-19 outbreaks.

[45] Examination with Acquire Executive
[46] Internal Department email
[47] Examination with former Department Contact Centre Performance Manager

126. According to an Acquire personnel manager, this program was used to recruit staff across all campaigns at Acquire, not just staff that were undertaking departmental work.[48] The same Acquire staff member told OVIC, 'we're constantly tapping into our existing network or staff to find referrals.'[49]

127. Acquire told OVIC that they believed the two subjects were recruited via the referral program.[50] No reference checks were conducted for Subject 1 and 2 and neither underwent a face-to-face interview.

What was the application process?

128. The application process for Acquire call centre workers recruited via a referral program was rapid during surge periods. It involved a phone interview during which candidates were asked about their recent work history and communication skills. They were also informed of the requirement to undertake a police check if their application was successful.

129. Upon conclusion of the call, applicants were offered a role if considered suitable. An Acquire personnel manager told OVIC that there was no written component included in the application process.[51]

130. Successful candidates were sent a welcome email. The welcome email sent to Subject 1 asked him to provide his address and date of birth for Acquire to 'create a profile in our database and set up an employment contract.'

131. Acquire also directed both Subject 1 and Subject 2 to bring 100 points of ID when they attended their first day at work in separate welcome emails.

132. In the case of Subject 1, the welcome email was sent at 12:23pm on 2 June 2021 to notify them that they would commence training at 12:00pm on 3 June 2021.

133. Subject 2 was sent a similar welcome email, although not identical. The email was sent on 21 July 2021 for a 23 July 2021 start. Subject 2's welcome email specifically mentions that they will 'be required to complete a police check consent form on the day'.

[48] Examination with Acquire Personnel Manager
[49] Examination with Acquire Personnel Manager
[50] Examination with Acquire Personnel Manager
[51] Examination with Acquire Personnel Manager

What pre-employment screening checks were performed?

134. Many employers undertake pre-employment screening to verify the identity and assess the character and qualifications of prospective employees.

135. The Victorian Public Sector Commission recommends all public sector organisations align their pre-employment screening policies and procedures with the Australian and New Zealand Standard on Employment Screening (Workforce Screening Standards).[52]

136. Probity, in the context of pre-employment screening, can be described as the 'level of integrity necessary to ensure the conscientious and honest conduct of one's working relationships and activities'.[53] Probity checks are one of the tools that employers use to verify the suitability of a person they intend to hire and can be essential to ensure potential employees meet the organisation's security requirements.[54]

137. The Workforce Screening Standards require the following elements to be checked to assess the integrity and credentials of candidates:

- curriculum vitae
- character references
- police records check
- conflict of interest
- declared academic qualifications
- employment references[55]

138. During the COVID-19 pandemic the Department and the engaged BPOs planned to implement a number of pre-employment screening steps to ensure the suitability of employees hired to undertake departmental work. These differed from the Workforce Screening Standards. They consisted of:

- phone screening interviews conducted by BPOs;
- statutory declarations in relation to criminal convictions, pending criminal charges, employment disciplinary actions and findings of improper or unprofessional conduct;

[52] Australian Standards, AS 4811:2022, Workforce Screening.
[53] Australian Standards, AS 4811:2022, Workforce Screening, 1.3.1.3.
[54] OVIC, IPP Guidelines, IPP 4 – Data Security, p 12, para 4.48.
[55] Australian Standards, AS 4811:2022, Workforce Screening, 2.8.5.3, 4 and 5.

- police check applications and checks; and
- confidentiality agreements.[56]

139. The Department also told OVIC that virtual face-to-face interviews were undertaken. Acquire staff told OVIC that when time permitted a longer phone interview or face-to-face interview might be undertaken. However during an outbreak where demand for staff was high the process involved a phone call then bringing staff in for onboarding.[57]

National Police Check

What is a National Police Check?

140. A National Police Check (police check) involves a search of a person's details, such as name and date of birth, against a centralised police index.[58] The outcomes of a police check are included in a certificate showing a person's any disclosable court outcomes, including charges, convictions and pending matters awaiting court hearing.[59]

141. A police check application needs to be lodged with an Australian police agency or an accredited body.[60] This application may be lodged by the employer or by the individual. The application must include certified identity documents of the person making the application.

What were the police check outcomes of Subject 1 and 2?

142. The Department confirmed that Subject 1 completed a police check application which was provided to the Department. However, the Department never submitted the application to be processed.[61]

143. Subject 1 has a previous criminal history including a conviction in 2018 for using a carriage service to menace.[62] The conviction resulted in a Community Corrections Order.

144. The prior conviction involved allowing a friend to log in to her Facebook account on Subject 1's phone. When she returned the phone, she had not logged out, Subject 1 then sent the friend

---

[56] Correspondence from Department to OVIC
[57] Correspondence from Department to OVIC
[58] Australian Federal Police, National Police Check, Frequently Asked Questions, available at https://www.afp.gov.au/what-we-do/national-police-checks.
[59] Victoria Police, National Police Certificates, available at: https://www.police.vic.gov.au/national-police-certificates
[60] Australian Criminal Intelligence Commission, Accredited Bodies, available at https://www.acic.gov.au/services/national-police-checking-service/find-out-more-information/accredited-bodies.
[61] Correspondence from Department to OVIC
[62] DPP v Awow, [2022] VCC 1353, Reasons for Sentence

photographs of herself with the caption 'look what I found- these photos may end up somewhere else'.[63]

145. Judge Ellis's Sentencing Remarks in relation to Subject 1's subsequent criminal offending note that there is a degree of similarity in the offending related to Breach 1 and Subject 1's earlier conviction in that another individual's information was accessed and then used in 'some sort of coercive or exploitative way.'[64] The Sentencing Remarks also note that Subject 1 was on bail at the time of the offending relating to Breach 1.[65]

146. Subject 2 also completed a police check application which was provided to the Department. However, the Department did not submit the application to be processed at this point. After the Department issued a direction to all BPOs on Friday 13 August 2021, the police check was submitted by Acquire on Wednesday 18 August 2021, more than three weeks after Subject 2 commenced employment on 22 July 2021 and after the breach involving Subject 1 was identified.[66] The police check was run, and the outcome received on 22 September 2021. The application took five weeks to be processed after it was submitted.

147. Subject 2 did not have a criminal history during the time they were employed at Acquire. Subject 2's employment was terminated on 26 August for failing to attend work. When Subject 2's police check was processed in September 2021, Subject 2 had two pending charges dated after their employment at Acquire had ceased.[67]

What happens if a police check is returned with a criminal history?

148. A clause in the services agreement with Acquire states:

> *Where the results of any probity and/or background checks or investigations undertaken in accordance with clause [redacted] reveal outcomes or other information that may be relevant as to whether it is appropriate for the relevant person to perform work or carry out the Contractor's obligations under this Agreement, the Contractor will disclose those results to the Department and will, if requested by the Department, prevent the relevant person from performing work or carrying out the Contractor's obligations under this Agreement.*[68]

149. This clause outlines that Acquire must notify the Department where the results of a probity check raise considerations about the appropriateness of the person to undertake departmental

63 DPP v Awow, [2022] VCC 1353, Reasons for Sentence.
64 DPP v Awow, [2022] VCC 1353, Reasons for Sentence.
65 DPP v Awow, [2022] VCC 1353, Reasons for Sentence.
66 Returned Police Check for Subject 2
67 Returned Police Check for Subject 2
68 Correspondence from Department to OVIC

work. It also requires that Acquire prevent the person from continuing to undertake departmental work if requested by the Department.

150. OVIC asked a senior HR representative at the Department to explain what the internal process was when a pre-employment police check is returned with a prior conviction.

> *A report is written and escalated to the deputy secretary of the business area to get their approval to continue with the employment or not. So there'll be an assessment made as to whether or not it will impact on the person's ability to perform their duties or whether it's something that actually makes them an unfit person to work in the public service, and a report will go to the deputy secretary for them to make the final decision about whether employment continues or not.*[69]

151. As would be expected, this response demonstrates the Department considers whether a criminal history will result in the employee being deemed unfit for work on a case-by-case basis.

152. Due to the serious nature of Subject 1's previous offending, the proximity of the offending and the fact that Subject 1 was on bail at the time of Breach 1, Subject 1 would have been considered unfit to work in this role by the Department.

Other pre-employment screening documentation required by the Department

Statutory declaration

153. A statutory declaration is a written statement by a person who declares that the information contained in the statement is true and correct in the presence of a witness.[70]

154. The Department required all new staff commencing at BPOs to sign a statutory declaration which included declaring they (I):

> *'do not have any charges laid against me by police concerning any offence committed in Australia or in another country in the past:*
>
> *do not have any offence/s of which I have been found guilty, committed in Australia or in another country in the past;*
>
> *do not have any disciplinary action taken against me by any current or former employer that led to the employment relationship ending, regardless of whether my*

[69] Interview with Department Director of People Services and Culture
[70] Department of Justice and Community Safety, Statutory Declarations, available at https://www.justice.vic.gov.au/statdecs.

> *employment terminated due to misconduct or that I resigned prior to the matter being concluded;*
>
> *do not have any findings of improper or unprofessional conduct by any Court or Tribunal of any kind; am not being or ever have been investigated by an employer, law enforcement agency or any integrity body or;*
>
> *similar in Australia or in another country;*
>
> *have provided the required four pieces of proof of identity and have submitted my completed police check consent form to COVID-hr@dhhs.vic.gov.au'*[71]

155. The Department informed OVIC that statutory declarations were used as an interim employment screening measure due to delays caused by COVID-19 (of up to five weeks) in police checks being processed and returned. This was because the rapid recruitment of staff needed for call centre functions meant that staff were required to start before their police checks could be submitted and processed. As the Director of People and Culture at the Department noted:

> *police checks can take some time and the provider at that time was having quite a lot of delays […].'*[72]

156. According to the breach review conducted by the Department following the second breach, statutory declarations were used as a means of bridging the gap between the commencement of staff and the return of the police check.[73]

157. Both Subjects had signed statutory declarations when they commenced their employment. The statutory declaration of Subject 1 was not truthful as it declared no criminal history or charges laid against him which was not accurate.

Confidentiality undertaking

158. The contract between the Department and Acquire required Acquire to ensure that each of its employees provide a confidentiality undertaking prior to accessing the Department's confidential information:

[71] Statutory Declaration signed by Subject 2.
[72] Interview with Department Director of People Services and Culture
[73] Department Review Report

> *The Contractor must:*
>
> *(a) procure from each person employed or engaged by it in relation to this Agreement an undertaking that is consistent with the Contractor's obligations under clause 7.1, in effect, that the person will not communicate, publish or release Confidential Information, before giving them access to any Confidential Information; and*
>
> *(b) on being informed, or otherwise becoming aware, of any breach or anticipated breach of any undertaking referred to in subclause (a), take such action as may be necessary to enforce that compliance, including all reasonable actions directed by the Department, and irrevocably authorises and permits the Department to enforce the undertaking in the event that the Contractor fails to adequately do so.*

159. Both Subjects signed confidentiality undertakings, which were provided to OVIC by the Department. Neither confidentiality agreement was dated but an Acquire personnel manager told OVIC that Agents were required to sign the document on their first day.[74]

160. The undertaking included the following clauses:

> *The Confidant will treat as secret and confidential all Confidential Information.*[75][76]
>
> *The Confidant will use the Confidential Information only for the purpose of its dealings with the Department (whether directly or indirectly).*[77]
>
> *The Confidant will not copy or reproduce Confidential Information without prior consent of the Department, will not allow any other person outside the Department access to Confidential Information and will take all necessary precautions to prevent unauthorised access to, or copying of Confidential Information in his or her control.*[78]

161. Both Subject 1 and Subject 2 signed identical confidentiality undertakings including the above clauses.

---

[74] Examination with Personnel Manager Examination
[75] Confidentiality Undertaking, Subject 1 and Subject 2, (undated).
[76] 'Confidential Information' means all information or data made accessible to the Confidant by the Department of Health and Human Services.
[77] Confidentiality Undertaking, Subject 1 and Subject 2, (undated).
[78] Confidentiality Undertaking, Subject 1 and Subject 2, (undated).

Findings

162. Given the Department indicated it required call centre staff urgently to handle increased volumes of calls following changes to health directions, the recruitment of staff by Acquire was undertaken in a hurried manner.

163. There was minimal vetting of staff taking place before they commenced work and began handling large volumes of personal and sensitive information as part of their role.

164. Normal recruitment processes and pre-employment screening such as reference checks, written applications, and face-to-face interviews were not conducted. Police checks were either not conducted at all or were completed after the person commenced work due to delays in processing time. To attempt to mitigate the risks associated with this, other measures were introduced in the form of confidentiality undertakings and statutory declarations from staff regarding criminal convictions and pending criminal charges.

165. The extreme operational pressures on the Department at the time it engaged Acquire cannot be doubted. The discovery of community cases of COVID-19 and the resultant new health directions created a massive increase in calls to call centres carrying out Departmental work. This required sufficient numbers of staff to meet the high demand.

166. However, while the operational pressures caused by the pandemic should not be minimised or forgotten, it must also be recognised that there were clear and significant risks in providing systems access to such a large cohort of rapidly onboarded agents without proper safeguards. That is, there were risks that unsuitable or ineligible staff sourced from external providers would be given access to personal information and would then misuse it.

167. It does not appear that these risks were sufficiently planned for, identified, or mitigated either:

- between the State of Emergency being declared and Acquire being engaged by the Department; or
- in the period after Acquire was engaged and the surge to call volumes had subsided.

168. Between the beginning of the State of Emergency and the engagement of Acquire by the Department, it was reasonable to foresee that there would be further outbreaks of COVID-19 and changes to health directions requiring additional call centre staff. It would have been appropriate for the Department to more proactively plan for the recruitment of call centre staff in such scenarios in a manner that allowed a greater level of pre-employment screening rather than taking the reactive approach it pursued.

169. This may have involved, for example, engaging Acquire sooner or at least making it known to Acquire that a future engagement could be forthcoming – and setting out minimum recruitment and pre-employment screening requirements. This could have given Acquire time to identify potential candidates and to carry out a more rigorous recruitment process.

170. In addition, it must be noted that subjects 1 and 2 were hired five and seven months respectively after the initial surge that required outsourcing to Acquire. This provided sufficient time for the Department to oblige Acquire to implement a more rigorous recruitment process than that which was adopted in January 2021. This did not occur, and both subjects therefore began handling personal information as part of their role within days of being recruited via an informal recruitment process.

171. The recruitment process that was implemented included a requirement for a police check to be conducted. Staff had to complete the relevant police check application form before commencing work and the check would be conducted after the staff member had commenced working. Given the lack of other probity measures, it was crucial that the application be processed as expediently as possible.

172. This did not occur, however. Both Subject 1 and Subject 2 provided completed police check applications when they began work at Acquire but the Department did not submit these to be processed.

173. No police check application was conducted for Subject 1 during his employment with Acquire. The police check application for Subject 2 was not processed until after the Department and Acquire became aware of Breach 1 and consequently discovered that police check applications were not being processed for Agents. Acquire then directly submitted the police check application for Subject 2, three weeks after they had commenced work. The reasons for these oversights are covered in greater detail in the report's discussion of theme 2 - responsibility and management of engagement with Acquire, including employee screening.

174. The lack of expedient submissions of police check applications meant that there was no mechanism to independently determine whether staff had a criminal history. Not having the results of a police check meant that the Department was relying solely on the word of those recruited that they had no criminal history as declared in their statutory declarations. This created unacceptable risk to personal information held by the Department as persons who had a relevant criminal history and lied about it would not be detected.

175. As such, the Department's handling of the police check process for both Subject 1 and Subject 2 was clearly inappropriate, with the consequences being particularly serious regarding Subject 1.

176. Neither Acquire nor the Department was aware that Subject 1 had a criminal history relating to the inappropriate use of personal information and was on bail at the time he was employed by Acquire. A police check of Subject 1 would have revealed a criminal history that would have precluded him from being employed to undertake departmental work – and from carrying out the criminal conduct which eventuated.

Does this amount to a breach of IPP 4.1?

177. Based on the above findings, the Deputy Commissioner is of the view that the Department contravened IPP 4.1 by:

- failing to ensure that externally contracted call centre staff were recruited in accordance with a sufficiently rigorous recruitment process with adequate pre-employment screening; and
- failing to submit police checks for contracted staff undertaking COVID-19 response work for the Department for a period of eight months, including:
  - i. failing to submit any police check in relation to Subject 1; and
  - ii. failing to submit a police check in an expedient manner in relation to Subject 2.

178. That is, in the circumstances, it would have been reasonable for the Department to have:

- planned ahead for the recruitment of call centre staff in outbreak scenarios in a manner that allowed a greater level of pre-employment screening;
- required Acquire to adopt a more rigorous recruitment process with adequate pre-employment screening in the period between the engagement of Acquire in January 2021 and Subject 1 and Subject 2 commencing work using departmental systems; and
- submitted police checks for Subject 1 and Subject 2 in an expedient manner.

179. In finding that the Department did not take reasonable steps to protect the personal information it held from misuse, the Deputy Commissioner has taken into the consideration the pressures faced by the Department in responding to an unprecedented and rapidly changing pandemic landscape.

180. However, this context does not render the steps taken by the Department reasonable for the purposes of IPP 4.1. The Department had previously experienced surges in operational demand and should have foreseen future surges prior to engaging Acquire in January 2021. Due to this elapsed time and accrued experience, it is reasonable to expect the Department to have had a more secure model for surging its workforce, whether externally contracted or not.

181. Additionally, the Department did not take steps to ensure that Acquire strengthened its recruitment and pre-employment screening process following the initial outbreak of COVID-19 community transmission that prompted the rapid engagement of Acquire in January 2021. The same process that was adopted in January 2021 was adopted in the recruitment of Subject 1 and Subject 2 in May 2021 and July 2021 respectively.

182. Regarding the issue of police checks, there is no evidence to suggest that it would be unreasonable to expect the Department to have submitted the relevant applications in an expedient manner.

183. Pivotal to the Deputy Commissioner's view that the Department failed to take reasonable steps to protect personal information from misuse is a consideration of the type of personal information to which staff at Acquire had access.

184. As demonstrated in paragraphs 61 and 65 above, contracted staff had access to systems containing a significant volume of personal information - both in total and in relation to each individual. The systems contained personal and sensitive information about thousands of individuals including but not limited to name, address, contact number, COVID-19 vaccination status and ethnicity. As such, the risk of harm from any misuse of such personal information was significant.

185. This is demonstrated by the significant harm suffered by the individual whose information was misused by Subject 1. Sentencing remarks describe that the offending had a profound effect on the victim to the extent that she has had to move states and is scared of being alone.[79]

After the breaches, both the Department and Acquire took steps to improve their onboarding processes.

- On 13 August 2021, the Department directed all BPOs to conduct police checks on current and future employees.[80] The former Manager Contact Centre Performance reported to OVIC that they met with all BPOs the afternoon the issue was uncovered. This is confirmed with several 'follow-up' emails in the following days between them and the BPOs confirming that the BPOs would be processing police checks for all current call takers and future hires.[81]

- On 13 October 2021, the Department provided OVIC with a breach report outlining the findings of an internal review and recommendations aimed at risk mitigation. This report recommends that the Department conducts a weekly review of 25 per cent of the outcomes of the police checks received by the BPOs. OVIC interviewed the person assigned this recommendation who confirmed that police check status for each BPO was reported to Department management every week following discovery of the breaches.[82]

[79] DPP v Awow, [2022] VCC 1353, Victim Impact.
[80] Department Review Report
[81] Emails sent to BPOs contracted by Department by the Contact Centre Performance Manager confirming police check process.
[82] Interview with Department Vendor and Contract Manager

Theme 2 - Responsibility and management of engagement with Acquire, including employee screening

Key Points:

- The Department first contacted Acquire on 1 January 2021 and Acquire began providing services on 2 January 2021. In line with the operation of the Department's Critical Incident Procurement Policy (CIPP), this engagement occurred outside standard procurement policies and practices.
- The Department and Acquire executed a services agreement in February 2021 which included a clause regarding responsibility for pre-employment screening.
- The clause required that, at the request of the Department, Acquire would be responsible for conducting pre-employment probity checks including police checks. From the commencement of the engagement with Acquire, the Department purported to take responsibility for collecting and processing police checks.
- The Department reviewed the process for submitting police checks after becoming aware of Breach 1. This revealed that, for a period of around eight months, police check applications were being forwarded to the Department by Acquire but were not being submitted by the Department for processing.
- This was likely due to the initial process of assigning responsibility for submitting police check applications being too informal. It was this lack of formality that resulted in no one at the Department identifying that the process was not being followed and police check applications were not being submitted.
- The services agreement was extended twice during 2021 before Breaches 1 and 2 occurred. These extension processes provided opportunity for the Department to review the contract and parties' adherence to their respective obligations, including pre-employment screening steps. However, the issue was not detected.

Who was responsible for pre-employment screening: the Department or Acquire?

Services agreement

186. The Department and Acquire signed a services agreement relating to their engagement on 11 February 2021, approximately one month after Agents began undertaking call centre work related to the Department's COVID-19 response.

187. A services agreement provides the parameters of the services arrangement between the contractor and the Department including:

- setting out the services being delivered and relevant activity descriptions;
- allocating the rights and obligations of the parties;
- identifying applicable Department policies and legislation;
- setting out the funding summary and payment schedule; and
- identifying the parties to the services agreement.

188. Responsibility for probity and pre-employment checks was included in the agreement between the Department and Acquire. The agreement states:

> *…if requested by the Department, the Contractor will at its own cost undertake probity and/or background checks or investigations on any person employed or engaged by the Contractor (including a volunteer) to perform work or carry out its obligations under this Agreement, including without limitation investigations as to criminal and police records (including National Security Clearance and finger printing). The probity and/or background checks or investigations required under this clause must be undertaken before the relevant person employed or engaged by the Contractor (including a volunteer) commences work under this Agreement.*

189. The agreement provides that at the Department's request, Acquire would be responsible for undertaking pre-employment screening checks, including criminal history checks and that the probity checks must be undertaken before the person employed begins work.[83]

190. However, this clause would only be activated if the Department requested that Acquire undertake this process. In the absence of such a request, the agreement does not specifically

[83] Services Agreement.

state which party would be responsible for pre-employment screening although the actions of the Department indicate that they were responsible.

191. OVIC did not obtain any evidence that suggested the Department requested Acquire to undertake police checks. On the contrary, OVIC found that the Department elected to undertake the collection and processing of pre-employment screening steps, including police checks and communicated that to Acquire. However, there appeared to be a lack of clarity around who was responsible for the police check process within the Department.

192. The Department provided OVIC with a copy of the requirements schedule, a document attached to the agreement outlining in detail the goods and services to be provided and forming part of the agreement. The requirement schedule states:

> *All new recruits to the services will be required to undergo a police check security clearance and complete a confidentiality agreement. The interim statutory declaration (police check) and confidentiality agreement must be received by the Department prior to commencement in training.*

193. This paragraph indicates that police checks, statutory declarations and confidentiality agreements were to be completed by new Agents and returned to the Department before they began training.

194. However, the wording of this paragraph of the requirements schedule is ambiguous and does not adequately specify if the documents to be returned to the Department include a completed police check application or a police check outcome. The requirements schedule is unclear and adds to the lack of clarity around the police check process.

Where did responsibility lie in practice?

195. In January 2021, when Acquire and the Department began their engagement but before the services agreement was executed, the Department elected to take responsibility for collecting and submitting police check applications for processing.

196. An email sent from a departmental operations manager to Acquire staff managers on 1 January 2021 indicates that the Department, and not Acquire, would collect the police check applications of new starters to submit for processing. The email reads:

> *'Below and attached is the process for police security clearance and confidentiality.*
>
> ***As part of the Department's onboarding process it is mandatory that you undertake our safety screening process. Please do not provide your own police check.***
>
> *Please follow these steps:*

> *1. Complete and sign the National Police check screening application (attached), providing addresses for the past **five** years*
>
> *2. Provide clear copies of your **four** pieces of proof of identity documents (these do not need to be certified). Details of the documents required are listed on the application form.*
>
> *3. Complete and sign the Confidentiality agreement (attached)*
>
> *4. Complete Interim statutory declaration (attached)*
>
> *5. Have the statutory declaration witnessed by an appropriate person (see attached list)*
>
> *6. If you are on a visa, please provide details.*
>
> *Please scan and return these to the Covid_19.HR@dhhs.vic.gov.au as soon as possible to fast track your onboarding.'*[84]

197. The above email also included an attachment for a Department of Health and Human Services National Police Check Application form. The email indicates that individuals seeking employment with Acquire were to complete the abovementioned documentation and email it to Covid_19.HR@dhhs.vic.gov.au.

198. The same email address for the former DHHS was also included in the statutory declaration forms of both Subjects. The statutory declaration states:

> *I declare that I have provided the requisite four pieces of proof of identity and have submitted my completed police check consent form to Covid_19.HR@dhhs.vic.gov.au*

199. According to a former senior departmental employee involved in contact centre operations, who will be referred to as Former Employee 1, Acquire was 'required to send details of those [onboarded] employees to the Department's COVID-19 human resources team using a position-based email account and that this team were responsible for managing the police check process.'[85]

200. This is also consistent with information provided by two employees at Acquire who noted that police checks were the responsibility of the Department.[86]

---

[84] Email from Department Director of Contact Centre Operations to internal Department staff
[85] Former Department Director of Contact Centre Operations Affidavit
[86] Examination with Acquire Personnel Manager; Examination with Acquire Operations Manager

> *I wasn't involved directly with those processes, but from my knowledge of - of seeing or hearing about it, it's - it's - our process of police checks was that from day one the Department of Health was responsible for police checks.*[87]

201. The investigation found that the Department was not submitting police checks for processing which were forwarded by Acquire for a period of eight months.[88]

202. It appears that at some point between February and April 2021, this process was altered such that instead of forwarding by email, 'Acquire started to input the employee names into a Dropbox file with a password instead of emailing them, and this file was not accessed.'[89]

203. The Department reported that:

> 'an administrative arrangement was established between the Department and BPOs for onboarding Agents, where the BPO would upload in a Dropbox of the Department for each Agent:
>
> - an application for a police check;
> - an interim statutory declaration in relation to criminal convictions, pending criminal charges, employment disciplinary actions and findings of improper or unprofessional contract; and
> - a confidentiality agreement[90]

204. Two Acquire staff interviewed by OVIC also confirmed that Acquire was directed to submit completed police check forms into a departmental Dropbox for processing.[91] OVIC could not find evidence to indicate who directed this change.

205. The Department did not access the relevant Dropbox folder while this process was in place and therefore did not submit the police check applications to be processed.

206. In interview, an Acquire staff member directly involved in operational matters confirmed that the process of the Department taking direct responsibility for submitting police check applications was not a standard practice for Acquire.[92] Rather, standard practice was for Acquire to directly submit police checks for processing for all staff and then assign Agents to campaigns.

---

87 Examination with Acquire Operations Manager
88 Department Review Report
89 Former Department Director of Contact Centre Operations Affidavit
90 Correspondence from Department to OVIC
91 Examination with Acquire Personnel Manager; Examination with Acquire Operations Manager
92 Examination with Acquire Personnel Manager

207. Nevertheless, Acquire staff reported that they had no reason to believe the Department was not submitting the police check applications.[93]

208. Both parties ultimately became aware that the police checks weren't being submitted after Breach 1. The Department provided OVIC with a review report that said that it undertook 'a review of the BPO contracts to confirm requirements around safety screening and police checks'. This review occurred between 6 August 2021 and 12 August 2021.[94]

209. The review uncovered that police checks had not been processed for four out of five BPOs contracted to the Department.[95] On 13 August 2021, the Department notified the four BPOs (including Acquire) that responsibility for submitting police checks would now be with the BPOs. As an interim measure, all call takers would be stood down until their police check had been processed.[96] The fifth BPO was exempt from this process due to a difference in the requirement schedule that required that BPO to process police checks from the onset of its arrangement with the Department.

What role did the Department's Human Resources play in this process?

210. OVIC gathered evidence suggesting the Department's human resources team was responsible for submitting police check applications in practice. However, this conflicts with an account provided by a senior departmental human resources staff member. Conflicting accounts of who was responsible for processing police checks indicates a lack of clarity and understanding around roles and responsibilities for the police check process within the Department.

211. On 1 January 2021, a senior departmental employee involved in contact centre operations sent an internal email to a number of departmental staff with the subject line 'HEADS UP – major onboarding about to commence'. The email assigned responsibilities for various induction activities for new staff commencing with Acquire and four other BPOs.

212. The email included an action item assigned to a senior employee in the Department's Human Resources team, to be ready to 'process police check stat decks and confidentiality agreements upon receipt of names – [Director of People Services and Culture]'.

213. Employee A, who was a recipient of the email, stated in interview that they did not remember the email as they were on leave at the time.[97] Employee A also stated:

[93] Examination with Acquire Operations Manager Examination
[94] Department Review Report
[95] Department Review Report; Correspondence from Department to OVIC
[96] Department Review Report
[97] Interview with Department Director of People Services and Culture

> *…when we hire people on our payroll we absolutely do the police checks, the stat decs and the confidentiality agreements but for people from other organisations that's not something we would've normally done so I don't remember that…*

214. Employee A also stated that 'the standard government contract actually has that the [Contractor] will do the police checks, and all the security checks, and just provide us [the Department] an assurance that that's been completed'.

215. While Employee A did not recall receiving the email, the email chain shows that Employee A forwarded the email to another Human Resources staff member, who they noted was acting in their role at the time, on the same day the email was received.

216. When asked why Employee A thought the police checks were not submitted for staff at Acquire, they stated:

> *my understanding is it was just an administrative error on their behalf, that possibly they were hiring people at a faster rate to try and meet the department's needs and that perhaps they were cutting corners to have things happen quickly, but that's just my conjecture.*[98]

217. Employee A's account of why police checks were note processed suggests that Acquire, and not the Department, were responsible for processing police checks for new Agents undertaking departmental work. Employee A's account conflicts with documentary evidence and accounts from other sources.

218. Former Employee 1, a former senior departmental employee involved in contact centre operations, stated:

> *It is my understanding that, as Acquire onboarded employees, they were required to send details of those employees to the Department's COVID-19 human resources team using a position-based email account and that this team were responsible for managing the police check process.*[99]

219. Another former employee from the Department also involved in contact centre operations, who will be referred to as Former Employee 2, said that:

> *prior to the first privacy breach, it was our understanding that each BPO would have every agent sign a stat dec which is something we have internally. And then our*

[98] Interview with Department Director of People Services and Culture
[99] Former Department Director of Contact Centre Operations Affidavit

> *internal HR person called [Director of People Services and Culture], was completing the actual police checks I believe.*[100]

220. The above evidence indicates that there was a lack of clarity within the Department about where responsibility lay for the pre-employment screening process.

How did the Department manage the engagement with Acquire?

221. Contract management is 'the systematic and efficient management of contract creation, execution and analysis for the purpose of maximising financial and operational performance and minimising risk.'[101] Contract management involves all contract related activities before, during and after the contract period and ensures parties to a contract meet their respective obligations.[102]

222. An internal review by the Department stated that 'the lack of contract management processes for the Acquire Contract allowed noncompliance with the police checks requirement to go unnoticed'.[103]

Contract variations

223. The initial services agreement between Acquire and the Department was for a period of three months, commencing on 2 January and ending on 2 April 2021. The agreement also included an option to extend the contract. This option was exercised, and the contract extended, on two occasions in 2021: from 2 April to 2 July 2021 and from 2 July to 31 December 2021.

224. A former senior employee in contact centre operations at the Department told OVIC that 'during the first renewal process which was June 2021, from memory, a formal review was adopted and overseen by a colleague [name omitted]'[104]

225. The two contract extensions that occurred in 2021 provided ample opportunity for the Department to review the contract and both parties' compliance with its obligations. This type of review process would have assisted the Department to identify the issue related to the submission of police checks at an earlier date.

---

[100] Examination with Former Department Contact Centre Performance Manager
[101] Buying For Victoria, Contract management and contract disclosure – goods and services policy, available at https://www.buyingfor.vic.gov.au/contract-management-and-contract-disclosure-goods-and-services-policy#rpl-skip-link.
[102] Buying For Victoria, Contract management – goods and services procurement guide, available at https://www.buyingfor.vic.gov.au/contract-management-goods-and-services-procurement-guide.
[103] Department Review Report
[104] Former Department Director of Contact Centre Operations Affidavit

Operational meetings

226. The Department and Acquire both reported frequent operational meetings between the two parties to discuss whether Acquire was meeting its contracted deliverables and key performance indicators.[105]

227. The Requirements Schedule which accompanied the services agreement stated:

> *A daily operational stand up will be held with all suppliers during periods of COVID outbreak where the services are experiencing peak demand*
>
> *A weekly operations meeting will be held with the supplier during Business as usual periods.*
>
> *A monthly Contract performance meeting will always be held with the Supplier.*

228. This indicates that there was frequent contact between Acquire and the Department in relation to the services provided under the agreement. The Requirements Schedule also notes the agenda items that would be discussed at these meetings, including:

> *c) Monthly contract and performance meetings*
>
> > *Power point pack detailing the month's performance inclusive of operational KPI's, attrition and focus areas for improvement*
> >
> > *Suggested initiatives regarding the service efficiency inclusive of people and process improvement, communications and technology opportunities.*
> >
> > *Contractual or commercial matters*

229. The above indicates that discussion of contract and commercial matters was an agenda item at the monthly meetings. This again provided opportunities for discussion not only of whether Acquire was meeting its KPIs and delivering the service it was contracted to do, but also review compliance with other requirements of the agreement.

230. According to Department Former Employee 2, who would attend daily operations meetings with staff from Acquire:

> *…we'd often have an operations meeting which would go for an hour where each provider – so we'd have an hour per contact centre provider where they would take us*

[105] Interview with Department Vendor and Contract Manager; Examination with Acquire Operations Manager

> *through their results which again would have me attending, [other performance management colleagues], and often the director who was responsible would also be part of that meeting.*[106]

231. A staff member in Acquire's operational unit told OVIC that these meetings included discussion of recruitment to the extent of numbers of staff available to undertake requirements. However, probity checks were not an agenda item until after the breaches occurred.[107]

232. Also consistent are reports on what was discussed within these operational meetings. Department Former Employee 2 reported that Acquire 'would take us through their results' during the daily meetings. That being, that the Department would ensure that Acquire was meeting its operational benchmarks of calls taken, length of call wait time and speed with which the calls were dealt with.'[108]

233. OVIC concluded that the Department had well-structured and frequent engagement with Acquire, however the focus of this engagement was heavily geared towards ensuring service delivery while neglecting to review adherence to other responsibilities such as probity checks, including the outcomes of police checks.

Findings

234. The investigation revealed multiple points where the Department did not appropriately manage its engagement with Acquire, and in particular, its screening of Agents.

235. Overall, it appears that, from the commencement of the engagement between the parties, the Department took ownership for collecting and submitting police check applications. There is nothing inherently inappropriate about the Department deciding to take responsibility for conducting police checks. However, the process that was implemented for doing so was unclear, generated confusion, and created circumstances where errors were foreseeable. The lack of mechanisms to oversee compliance with pre-employment screening obligations then meant that those errors were not detected.

236. The initial process of assigning responsibility for submitting police check applications was too informal in that there was no documentation, checklist, follow-up communication, or process for evaluating the appropriateness of the system put in place. While the speed with which Acquire was engaged necessitated for processes to be set up quickly, the lack of formality meant that no one at the Department identified that the process was not being followed and police check applications were not being submitted.

---

[106] Examination with Former Department Contact Centre Performance Manager Examination
[107] Examination with Acquire Personnel Manager
[108] Examination with Former Department Contact Centre Performance Manager Examination

237. The services agreement and requirements schedule that was negotiated following the initial period of informal engagement was inconsistently interpreted by staff within the Department. This investigation therefore found that the contract did not fulfil its purpose of clearly assigning responsibilities between the two parties with relation to probity checks. Had this been established more clearly the failure to submit the police check applications may have been more obvious.

238. While the services agreement and requirements schedule both refer to pre-employment screening, the relevant provisions are ambiguous and lack specificity. This created confusion about where responsibility lay for submitting police check applications, as evidenced by the inconsistent interpretation of who was responsible for pre-employment screening within the Department. While it is clear that the Department took responsibility for processing police checks and did not do this, the lack of clarity in the agreement may have contributed to uncertainty around roles and responsibilities within the Department.

239. In fact, this confusion remained even after the Department became aware that police check applications were not being submitted. The Department provided a review report to OVIC following Breach 2 which noted that 'the initial procedure was substantially different from the procedure set out in the Acquire Contract'. This interpretation is also inconsistent with the wording of the services agreement. The agreement states that, *if requested*, the contractor would be responsible for conducting police checks. OVIC did not collect any evidence to suggest the Department ever requested Acquire take responsibility for this process until after breach 1.

240. The lack of contract management mechanisms to systematically review parties' adherence to all contractual obligations, including pre-employment screening steps, then meant that the issue remained undetected.

241. While the Department and Acquire had a well-structured and extensive engagement, this engagement was geared towards ensuring service delivery and did not consider the full spectrum of obligations required under the agreement. Had the Department implemented sufficient contract management mechanisms aimed at reviewing parties' adherence with the entire agreement, instead of just parts of it, the issue of non-submission of police check applications would have been detected. Further, probity screening plays an important role in ensuring that only appropriate people are given access to personal information. It is the view of the Deputy Commissioner that it is reasonable to expect that the operational meetings would include agenda items relating to personnel security, including processing and outcomes of pre-employment screening checks.

242. In other words, it should have become clear between the commencement of the engagement and becoming aware of Breach 1 that no police check outcomes were being received. This should have prompted a review of which party had responsibility for submitting the police check applications pursuant to the contractual arrangements and how this was being implemented in practice. Such a review would have revealed that the Department had this

responsibility but was not meeting its obligations. Expedient remedial actions should then have followed.

243. This is especially the case given the services agreement was extended twice during 2021. These extension processes provided opportunities for the Department to review the contract and parties' adherence to their obligations.

Does this amount to a breach of IPP 4.1?

244. Based on the above findings, the Deputy Commissioner is of the view that the Department did not take reasonable steps to protect personal information it held from misuse, and therefore contravened IPP 4.1.

245. There was a clear risk of misuse of personal information and consequent harm to individuals. Agents had access to systems containing a significant volume of personal information - both in total and in relation to each individual. The systems contained personal and sensitive information about thousands of individuals, including but not limited to name, address, contact number, COVID-19 vaccination status and ethnicity.

246. This risk was heightened by the lack of probity checks conducted on staff before they commenced working with Acquire and accessing departmental systems – as discussed in the section on Theme 1 above. In this context, it was crucial to conduct expedient police checks to mitigate the risk of personal information being misused.

247. With regard to pre-employment screening and the submission of police check applications, it would have been reasonable for the Department to:

- formally establish and clearly communicate the respective roles and responsibilities of the Department and Acquire from the beginning of the engagement;
- clearly and unambiguously define the respective roles and responsibilities of the Department and Acquire in the services agreement that was executed between the parties;
- establish sufficient contract management mechanisms once the services agreement had been executed to enable ongoing review of parties' adherence to their obligations regarding the submission of police checks; and
- implement checks to ensure the person, team, or division responsible for processing the probity checks was undertaking this role.

248. Taking such steps would not have been disproportionately onerous for the Department, even when considering the context of the pandemic response. Establishing greater clarity on respective responsibilities at the point of initial engagement and within the services agreement would not have imposed a significant resource burden.

249. Similarly, as noted above, the Department was already contributing resources to ongoing engagement with Acquire in overseeing operational performance. Reviewing each party's compliance with contractual responsibilities as part of this engagement would not have necessitated a significant addition of resources.

Steps taken by the Department after the breaches:

- On 13 August 2021, the Department notified Acquire that responsibility to submit police checks was now with Acquire. The evidence provided to OVIC indicates that this was communicated in a meeting attended by staff from both Acquire and departmental operational units. This meeting was then confirmed in a follow-up email that states 'Acquire will conduct a national police check for all active/existing DH staff' and 'Acquire will pick up the completion of police checks for all new DH staff'.[109] Acquire call takers were stood down while their police checks were being processed. The status of the police checks submissions was discussed in frequent stand-up meetings and Acquire agreed to a monthly audit of the progress.

- On 15 February 2022, a new requirement schedule was confirmed between the Department and Acquire. This document clearly sets out that Acquire must 'take reasonable steps to assess the suitability of any person applying to work for the Contractor including as either an employee or subcontractor', including 'undertaking the probity and background checks' as set out in the services agreement between the party. The new requirement schedule formalised the allotment of responsibilities, although Acquire was undertaking police checks of Agents since August 2021.

- On 10 March 2022, the Department issued a Variation of Agreement of the contract with Acquire that implemented several measures aimed at mitigating the risks revealed by these breaches. These changes included the addition of several privacy related clauses which dictate Acquire's responsibilities when accessing Department held information with relation to confidentiality and privacy. The Variation adds clauses to:

    - govern Acquire's collection, storage and disclosure of personal information gathered from or on behalf of the Department, and
    - ensure Acquire notify the Department of any security incident, take reasonable steps to remediate the issue and comply with all reasonable steps the Department requests during the incident.

[109] Departmental internal emails

Theme 3 - Data management systems and training

Key points:

- The Department's data management system had a range of security measures in place, including individual user login credentials, system logs and multi-factor authentication.
- The multi-factor authentication system used on the data management system required users to have their mobile phone with them. This meant that Agents conducting departmental work needed to have their phone with them while working.
- The method of multi-factor authentication (MFA) implemented reduced the effectiveness of Acquire's ability to enforce a no-phone policy. However, the Department reported that there were no alternative methods of MFA that were feasible in the circumstances.

Background

250. The systems and information to which contracted staff had access are referenced above at paragraphs 61 and 65.

251. OVIC understands that Subject 1 had taken a photo of the victim's Genesys profile.[110] On 24 July 2021, when Subject 1 impersonated an Authorised Officer, he reportedly showed the victim that he had her personal information on his phone. As such, when Subject 1 arrived at her house he used his access to this personal information from a departmental system to lend credibility to his claim to be an Authorised Officer.

252. At the time of Subject 2's arrest, they were found to have a photo on their phone of a computer screen displaying an address. OVIC concluded that the photo was of CVMS based on the following information:

- Image metadata indicated it had been taken in the vicinity of the Acquire office at 11:53am on 25 July 2021.[111]
- Subject 2 was active in the Genesys system to conduct departmental duties from 8:53am to 3:45pm on 25 July 2021.[112] This was only their second day of conducting work using departmental systems.

[110] Examination with Former Department Contact Centre Performance Manager Examination, Systems demonstration provided to OVIC by Department.
[111] Photo provided to OVIC by Victoria Police
[112] Genesys logs of Subject 1 and Subject 2.

- Information obtained during the course of the investigation indicated that Subject 2 had searched the address that was captured in the photo.[113] CVMS is the only system that staff had access to that was able to be searched.

- A system demonstration provided to OVIC on 4 May 2022 by the Department confirmed that the visual layout of the fields on the CVMS system matched that of the photo found of Subject 2's phone.

What technical controls were implemented to protect information held on departmental systems?

Multi-factor authentication and use of mobile phones

253. Multi-factor authentication (**MFA**) is a security method requiring two or more proofs of a user's identity to gain access to a website, application, or database.[114] MFA provides significantly more security and protection to systems as it makes it harder for adversaries to access sensitive information.[115] This method is often used by organisations to ensure that only authorised individuals can access certain systems or information.

254. Organisations can employ MFA in a number of ways. MFA requires the combination of at least two types of information, for instance a password or pin and a fingerprint scan. Some MFA options include:

    - Physical token
    - Random pin
    - Biometrics / fingerprint
    - Authenticator app
    - Email
    - SMS

255. The Department used the Microsoft Authenticator App installed on the mobile phones of Agents as the second form of identity in the MFA process. This meant that, in addition to entering their login credentials (including password), staff would then be required to verify their

[113] Documents provided to OVIC by Victoria Police.
[114] Australian Government, Australian Cyber Security Centre, Multifactor Authentication, available at: https://www.cyber.gov.au/mfa.
[115] OVIC, IPP Guidelines, p 13, available at: https://ovic.vic.gov.au/wp-content/uploads/2019/11/IPP-4-2019.B.pdf; Australian Government, Australian Cyber Security Centre, Multifactor Authentication, available at: https://www.cyber.gov.au/mfa.

identity through the Microsoft Authenticator App or via SMS on their mobile phone before being able to access departmental systems.

256. As a result, staff were required to have their mobile phones with them in order to gain access to departmental systems and undertake their roles.

257. Acquire's Electronic Device Policy required that Agents not use their mobile phones in operations and training areas.[116] However, implementing this policy was not possible for staff undertaking departmental work due to the requirement for MFA via the Microsoft Authenticator App downloaded to staff phones or via SMS.[117] During an examination, a personnel manager at Acquire told OVIC;

> *A: To be completely candid it's not something that we enjoy because we'd prefer the staff members have their phones in lockers off the floor[…]*
>
> *Q: Is that a policy or is that just a preference that apply?*
>
> *A: That is one of our policies, yeah, that mobiles aren't to be used on the floor but obviously with the Department of Health it needs to be different given there's two-factor authentication for everyone on that campaign.[118]*

258. Acquire staff knew that the use of phones for the purposes of MFA created risks to information. In interview, a the same Acquire personnel manager stated that:

> *[…] I guess if someone's got their phone on their desk there's always a risk that, you know, an Instagram notification might go off and someone might check that and that's of course not what we want. So there's definitely a risk there.[119]*
>
> *[…] having mobiles on the floor would obviously be a risk and sometimes, you know, if bad people can do bad things it's difficult to … police that at all times […]*

259. Acquire staff reported to OVIC that they raised concerns with the Department about the use of mobile phones to access systems. In response to raising those concerns, they said they were told by the Department that accessing the system required phones.[120]

260. Acquire also installed lockers in the office for Agents to store their phones once they had logged into the systems in an attempt to mitigate risk.[121]

---

[116] Examination with Acquire Personnel Manager; Acquire Electronic Device Policy.
[117] Examination with Acquire Personnel Manager.
[118] Examination with Acquire Personnel Manager.
[119] Examination with Acquire Personnel Manager.
[120] Examination with Acquire Operations Manager Examination.
[121] Examination with Acquire Operations Manager Examination.

261. The Department told OVIC that it considered whether MFA could be undertaken via alternative means such as through email. The Department told OVIC that it could not make this change as it would affect all users of CVMS, not just contact centre staff. It also noted that nurses and other frontline staff would not be issued a health services email address, therefore there would be no email address that the authentication code could be sent to.[122]

How were new Agents trained to undertake departmental work?

262. Initially, Department staff trained Acquire team leaders through a 'train the trainer' model.[123] This involved staff from the Department walking the Acquire team leaders through the training material which they would then, in turn, deliver to their teams.[124]

263. According to Acquire staff, the training provided to Agents on how to undertake their roles initially consisted of largely scenario-based exercises in relation to call-taking, including instruction on how to manage calls with distressed individuals.[125] However, it was noted that the training provided by the Department did not depict the types of calls Agents would be likely to receive and was not 'tailored enough for the types of calls we were getting.'[126]

264. An email sent from the Department to Acquire managers on 1 January 2021 indicates that training provided to Acquire team leaders would be two and a half hours:

> *'We have confirmed training will be 2.5 hours. The DHHS will provide a trainer to facilitate this session with ongoing training to be provided by Acquire as required.'*[127]

265. The Operations Manager at Acquire reported that the systems training provided to Agents was about four hours.[128] Acquire staff told OVIC:

> *It just felt like almost, get people in, read this bit out, show them some, you know, a PowerPoint presentation, and then get them on the phones.*

266. An Acquire staff member also told OVIC they raised concerns about the level of training provided to Agents with a senior Contact Centre Operations staff member at the Department when the campaign with Acquire was first launched.[129]

---

[122] Interview with Department Staff
[123] Examination with Acquire Operations Manager
[124] Examination with Acquire Operations Manager
[125] Examination with Acquire Operations Manager
[126] Examination with Acquire Operations Manager
[127] Internal department email from Director of Contact Centre Operations to Department staff.
[128] Examination with Acquire Operations Manager
[129] Examination with Acquire Operations Manager

> *Well, yeah, I guess, um, you know, my sort of question was, hey look, is there anything else? Is this it, is this the pack, or is there anything else that we can supplement? Could we - you know, can we set up more sessions and what can we do? And it was kind of like, well look, that - that's what we've got, that's - that's what we use ourselves, so you know, it should be enough.*[130]

267. Acquire employees also reported to OVIC that the company's usual level of training differed depending on the type of campaign the Agent would be working on, but stated:

> *In most cases, we'd prefer training to be running from anywhere from three to eight weeks.*[131]

268. The shortened training regime was reportedly done with the aim of getting Agents accepting calls as quickly as possible.[132]

269. Acquire reported that 'a day's training is perhaps very green to be getting people onto the phones so, yeah, I guess any every line operation has probably had reservations over the journey'[133].

Findings

270. It was an appropriate step for the Department to implement MFA for accessing relevant systems. Given the volume and sensitivity of the personal information on the systems, it was critical to reduce the risk of third parties gaining unauthorised access to these. If only one layer of authentication had been used and one user's login credentials were compromised, a malicious third party could potentially have accessed the totality of the information on the systems.

271. It was also appropriate that Acquire had a policy forbidding the use of mobile phones by staff when in areas where work was being conducted.

272. There will always be difficulties when trying to completely enforce a no-phone policy as individuals motivated by malicious intent can attempt to circumvent measures to police such a policy – either by using their phone or using other ways to inappropriately record information. This is particularly the case where there is a lack of probity in the recruitment of such individuals, as was the case in the present circumstances.

[130] Examination with Acquire Operations Manager
[131] Examination with Acquire Personnel Manager
[132] Examination with Acquire Operations Manager
[133] Examination with Acquire Personnel Manager

273. Unfortunately, the method of MFA that was implemented by the Department – which required the use of staff mobile phones – reduced Acquire's ability to effectively monitor and enforce its no-phone policy even further.

274. It would clearly have been preferable to have used a method of MFA that did not require the use of mobile phones. This would have reduced, though not eliminated, the risk of mobile phones being used to capture personal information for nefarious purposes. Ideally, the Department could have considered alternative MFA measures, such as tokens, as a risk management exercise before the emergency began.

275. However, given the same method of authentication applied to all users of CVMS, there were overarching practical considerations that weighed against using a different form of MFA.

276. Once the pandemic had begun, changing to other MFA methods would have disproportionately hindered the urgent work of other users – such as those frontline workers involved in the administration of vaccinations. Removing the use of MFA to reduce the risk of misuse of mobile phones would have created greater risks to individuals' privacy than it would have alleviated.

277. The training provided to Acquire Agents was limited and not consistent with the standard practices of Acquire which would have normally required further training. Training provided to Agents regarding appropriate handling of personal information was minimal due to the time-critical aspect of their roles.

278. It is acknowledged, however, that Agents were made aware of the need to appropriately handle departmental information as part of their roles. The Confidentiality Undertakings signed by both Subjects 1 and 2 set out the requirement to keep information confidential and only to use information for the purposes of their role. It is therefore unlikely that additional training would have prevented them from carrying out Breaches 1 and 2.

Does this amount to a breach of IPP 4.1?

279. Based on the above findings, the Deputy Commissioner is of the view that the Department did not contravene IPP 4.1 in relation to its data management systems and training.

280. The implementation of multi-factor authentication was a reasonable step to take to protect personal information on departmental systems from misuse as well as from unauthorised access, modification and disclosure.

281. While the method of MFA that was implemented reduced the effectiveness of Acquire's ability to enforce a no-phone policy, it does not appear that alternative means were feasible in the circumstances – taking into account the issues this would pose to other aspects of the Department's pandemic response.

282. The Deputy Commissioner considered the operational difficulties posed by other methods of MFA against their likelihood of protecting personal information from the eventual misuse that

occurred. The lack of pre-employment screening conducted on Subjects 1 and 2, as discussed above, greatly heightened the risk of misuse of personal information. The implementation of MFA in a manner that would not require the use of a mobile phone would not have reduced this risk to an extent great enough to warrant the operational issues it would have caused at the time.

283. Although the circumstances in which phone-based MFA was inappropriate might have been foreseen, the Deputy Commissioner considers that during the pandemic the implementation of MFA in a manner requiring the use of a mobile phone did not constitute a contravention of IPP 4.1.

284. With regard to training, more time and emphasis should have been dedicated to appropriate handling of personal information. However, the Deputy Commissioner is satisfied that it would have nevertheless been abundantly obvious to Subjects 1 and 2 (and to other Agents) that misusing personal information in the manner they did was clearly inappropriate.

285. As such, the Deputy Commissioner does not consider the level of training provided to Agents constituted a contravention of IPP 4.1.

Steps taken by the Department and Acquire after the breaches:

- The Department had previously explored altering the processes of multi-factor authentication for both CVMS and Genesys. The proposed change was for the unique code to be sent to an email instead of a mobile phone, removing the risk of needing phones near desks. According to the systems administrators interviewed by OVIC, this was not possible as 'it would affect all users, not just the contact centre staff'.[134] This would mean that vaccine providers and other health care providers would access the system through an email address. According to the CVMS system administrator, this change to MFA wouldn't reduce risk of users taking photos of a computer screen, particularly considering that many of these users would access their emails through their phone.[135]

- In the updated Requirements Schedule between the Department and Acquire, there were several management requirements set out. For instance, there must be an advisor to team leader ratio that is not more than one to fifteen.[136]

- Acquire reported to OVIC that they had significantly changed the training that was provided to Agents.[137] According to the Acquire Operations Manager, "along the journey we changed that training to be a lot more involved because we felt that it wasn't strong enough in terms of what the candidates were learning or going through'.

[134] Interview with Department IT Staff.
[135] Interview with Department IT Staff.
[136] Requirements Schedule
[137] Examination with Acquire Operations Manager

Whether to issue a compliance notice

286. Under section 78(1) of the PDP Act, the Deputy Commissioner may issue a compliance notice on an organisation if satisfied that the organisation has committed a serious, flagrant, or repeated contravention of the IPPs. A compliance notice requires an organisation to take specified action within a specified period for the purpose of ensuring compliance with the IPPs.[138]

Were the contraventions 'serious'?

287. The Deputy Commissioner considered the following factors, as set out in OVIC's Regulatory Action Policy,[139] in determining whether the contraventions of IPP 4.1 were serious for the purpose of s 78(1)(b)(i) of the PDP Act:

- the type of information involved, for example whether sensitive or delicate information is involved;
- the amount of information involved and the number of people that it relates to;
- whether particularly vulnerable or disadvantaged groups are affected;
- the extent of harm to individuals and the likelihood of that harm eventuating; and
- the impact the breach has on public trust.

288. The Deputy Commissioner determined that the contraventions in question were serious. The relevant Department systems contained a very large volume of personal information - both in total and in relation to each individual.

289. They contained both sensitive and delicate information, and the risk of harm from any misuse of such personal information was significant – as demonstrated by the significant harm suffered by the individual whose information was misused by Subject 1.

290. In addition, the contraventions of IPP 4.1 and the risk of misuse of personal information (such as those set out in Breaches 1 and 2) had the potential[140] to seriously erode public trust in and the public's willingness to cooperate with the government's pandemic response.

[138] PDP Act, s 78(2).
[139] OVIC, Regulatory Action Policy 2022.
[140] The public did not become aware of the circumstances of the circumstances of Breach 1 until media reports in August 2022.

Decision not to issue a compliance notice

291. While the Deputy Commissioner is satisfied that the contraventions of IPP 4.1 were serious, she does not view a compliance notice as the most appropriate course of action in the circumstances. Rather, she has decided to issue a number of recommendations.

292. Where a compliance notice is issued, it requires an organisation to take 'specified action' within a specified period.

293. However, noting Victoria's transition from the pandemic response, the Deputy Commissioner considered the risks of future non-compliance with IPP 4.1 not in relation to the COVID-19 pandemic context, but in terms of future emergency scenarios.

294. As such, the issues the Deputy Commissioner identified as needing to be addressed are necessarily broad in nature. That is, the investigation identified a need for the Department to ensure its emergency management planning includes the identification and mitigation of risks posed to information privacy during times of crisis.

295. It would therefore be inappropriate and ineffective for the Deputy Commissioner to direct the Department to take specific actions to address these issues, especially in the complex context of emergency management planning.

296. The Deputy Commissioner therefore decided to issue the Department with recommendations to ensure that the risks identified in this investigation are properly considered within the Department's emergency management planning.

297. The recommendations have intentionally placed responsibility on the Department to determine the specific actions required to implement them within its own internal review of its emergency management plans and procedures.

298. The Deputy Commissioner also took into consideration the Department's engagement with OVIC during this investigation, and her belief that the Department views these breaches as seriously as she does. As such, she expects that the recommendations will enable the Department to action these recommendations as a matter of urgency, with appropriate oversight from OVIC.

299. The Deputy Commissioner expects an update from the Department by the end of March 2024 on the action it has taken or plans to take to implement the recommendations.

Recommendations

300. The Deputy Commissioner recommends that the Department of Health reviews its emergency management planning policies and procedures to ensure they adequately address the following:

1. Preparedness for the recruitment of surge workforces which adequately considers and mitigates associated privacy risks including:

    a. the risk of ineligible or unsuitable externally contracted staff gaining access to personal information held by the Department (this may include, for example, contingency planning for expedited police checks, and the development of minimum recruitment and character standards to be adhered to by contracted service providers); and

    b. the need to review appropriateness of access controls to Department systems for externally contracted staff.

2. Assignment of responsibility to a senior department employee (reporting directly to the Secretary) to ensure that, for contracts executed with contracted service providers associated with emergency management response, there is appropriate:

    c. contract creation – responsibility for obligations relating to the protection of personal information is clearly and appropriately assigned between the Department and the contracted service provider; and

    d. contract management – adherence by both parties to obligations relating to the protection of personal information, which is systematically reviewed and verified.

Annexure A

DEPARTMENT'S RESPONSE TO REPORT

14 JULY 2023

1. This document provides the response of the Department of Health (**Department**) to the report prepared by the Deputy Commissioner of the Office of the Victorian Information Commission (**OVIC**) on her investigation into misuse of Department of Health information by third party employees during the pandemic response (**Report**).
2. The investigation was conducted pursuant to the Information Commissioner's powers under section 8C(2)(e) of the *Privacy and Data Protection Act 2014 (Vic)*.

A. FINDINGS

3. The Department accepts the Deputy Commissioner's finding that it breached IPP 4.1 and acknowledges that the contraventions are of a serious nature. The Department takes its information privacy obligations very seriously and has cooperated openly and responsively to assist the Information Commissioner in conducting the investigation of the misuse of information by third party employees that are discussed in the Report.

4. The Department deeply regrets that private information was able to be misused by a third-party employee with access to the Department's call centre system and acknowledges the profound impact of this.

B. RELEVANT CONTEXT

5. While the Report acknowledges the substantial pressures the Department faced in responding to an unprecedented and rapidly changing pandemic landscape and seeks not to minimise this context, it finds this did not render the steps the Department took reasonable for the purposes of IPP 4.1. The Department accepts that more could have been done to protect the privacy of Victorians.
6. The Report suggests that, based on operational demands posed by the pandemic before January 2021, the Department should have had a more secure surge workforce model in place and should have engaged earlier with potential contracted service providers to allow time for identification and screening of potential candidates. This suggestion, respectfully, does not sufficiently appreciate and recognise the magnitude of the challenges in pre-planning a surge workforce nor the limitations on advance pre-screening where it is not known when those resources will be required.
7. After the Department's experience with the early COVID-19 variants, it was indeed predictable that more variants of concern would emerge in future, but exactly when this would occur, and the extent on case numbers, was always unpredictable.
8. In addition, the Chief Health Officer's health directions to deal with emerging threats guided the measures that the Department would take to protect public health, including the engagement of third-party service providers to assist in the response. The content of the directions and their application was very much dependent on the epidemiology and circumstances at that time, and not pre-determined in advance.
9. The Report acknowledges that the volume of calls to the call centres staffed by the third-party employees was largely dependent on the nature of Chief Health Officer directions in place. For instance, from 1 January 2021, the Victorian Border Crossing Permit Directions meant that call centres were very quickly flooded with inquiries. These unprecedented call volumes were then surpassed by inquiries and bookings as vaccinations became available with about 1 million calls in one day.

1

OFFICIAL: Sensitive

10. The threat of COVID-19 outbreaks while Victorians were not fully vaccinated and new variants of concern which resulted in increased transmission required a rapid and elevated response, including border closures and the use of external surge workforces to help manage contact tracing and other pandemic response work. The urgency for getting third- party surge workforces in place at that time cannot be underestimated. The time available for pre-screening was very restricted – when the Department knew a wave had started it was already too late.

11. As new variants emerged (especially Omicron) and impacted Victorians in different ways, the COVID-19 response required constantly adapting approaches, agility, and surge capability at a time when workforces were facing multiple demands, fatigue and illness requiring furloughing. I suggest that the Report may be interpreted to imply that planning for and responding to the pandemic is static and predictable, with 'downtime' to review and audit processes. This was simply not the case. The COVID-19 urgency and changing context did not allow this in the way that would have been done in ordinary circumstances.

12. While acknowledging the benefits of seeking to identify and pre-screen surge workforces in advance of their need arising, such surge models have limitations. It can be both expensive and impracticable to pre-screen candidates to be employed on short notice. This can be particularly acute where resources are in demand generally due to the emergency scenario across the health sector, and other opportunities for work may mean those pre-screened staff are no longer available. It was also not practical to rely on normal recruitment processes and pre-employment screening, especially where processing delays were inevitable. At the relevant time, due to the impact of COVID-19, police checks were taking up to 5 weeks.

13. Therefore, the urgent utilisation of third-party service providers, at scale, was necessary for the Department to fulfil its obligation to protect the lives of Victorians. The rapid and massive uplift in contact tracing capability afforded through the third-party staffed call centres enabled Victoria to return to zero cases on multiple occasions. This achievement remains unique in the world, particularly for the Delta variant, and an achievement that unquestionably saved lives, likely thousands of lives.

14. So, while the Department accepts that more should have been done to protect the privacy of Victorians and deeply regrets that the system was able to be misused by a third-party employee, I would hope that you appreciate and accept that, at that time, it was correct for our efforts to be focussed on disease transmission containment and protecting the lives of Victorians.

C. MITIGATIONS/CONTINUOUS LEARNING AND IMPROVEMENT

15. The Department is committed to using the lessons learned from COVID-19 to strengthen and improve Victoria's pandemic and emergency management response and welcomes the recommendations of the Deputy Commissioner. As noted in the Report, since the information misuses that were the subject of the investigation the Department made several improvements to clarify responsibility for pre-employment screening and checks with the contractor to mitigate risks. These included:

    - notification that responsibility for police checks rested with the contractor and that all active and new staff required completed checks before continuing or commencing work.
    - improved on-boarding processes following internal review, including the Department conducting weekly audits of police check outcomes received from the contractor.

- implementation of a new requirements schedule which clearly documented the third-party contractor's obligations to take reasonable steps to assess the suitability of any person applying to work for them including undertaking probity and background checks.

16. The Department deeply regrets that private information was able to be misused by a third-party employee with access to the Department's call centre system and acknowledges the profound impact of this.
17. The systems the subject of the misuse have been either decommissioned or are not being used by contracted service providers as they are no longer conducting contact tracing or COVID-19 immunisation appointment bookings.

D. RECOMMENDATIONS

18. The Department thanks the Information Commissioner for the recommendations and notes these are intended to ensure that the broad issues identified during the investigation are properly considered within the Department's emergency management planning.
19. The Department is committed to embedding everything it has learned throughout the COVID-19 pandemic into its future emergency management response. It will ensure that its emergency planning and procedures include the identification and mitigation of risks posed to information privacy during times of crisis. The Department will carefully consider the recommendations to determine the specific practicable action to implement consistent with their intent.
20. The Department will provide the Information Commissioner with an update by 1 March 2024 on the action it has taken or plans to take to implement the recommendations, where not already implemented and where practicable.

www.ovic.vic.gov.au