OVIC

Office of the Victorian Information Commissioner

Unauthorised access to client information held in the CRISSP database

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

Table of contents

Foreword

In December 2018, the Department of Health and Human Services (**DHHS**) notified my office of an incident involving unauthorised access to one of its information systems. The system was accessed by a person, referred to as 'XYZ'[1] in this report, who was formerly employed by a contracted service provider (**CSP**) of DHHS and whose access privileges had not been revoked on his departure.

The Privacy and Data Protection Deputy Commissioner commenced an investigation to determine how XYZ had retained his access to the system and whether, in failing to rescind that access, DHHS or the CSP had breached the Information Privacy Principles in the *Privacy and Data Protection Act 2014*. This report details the findings of that investigation. The investigation ended in May 2020, but OVIC decided not to publish this report until now, due to the criminal investigation and trial of XYZ for matters that were not the subject of the investigation.

The Deputy Commissioner found that both DHHS and the CSP contravened the IPPs and issued a compliance notice against DHHS. Both the CSP and DHHS committed to implementing the recommendations made by the Deputy Commissioner and the terms of the compliance notice.

The CSP has implemented the recommendations made to it and DHHS (now the Department of Families, Fairness and Housing) is on schedule to complete all the specified actions required by the compliance notice. Both organisations cooperated fully with the Deputy Commissioner's investigation and demonstrated a willingness to improve their practices and learn from the incident. They recognised the incident's gravity and responded appropriately.

This incident has important lessons for all organisations, particularly those that deliver services through contracted service providers, and share personal information with those providers and their employees.

Outsourcing arrangements cannot be 'set and forget'. When a government agency shares personal information and system access with its contractors, the agency retains both a legal and a moral duty to protect the personal information it collects, uses, holds, and discloses. Government organisations can outsource the management of a program, but they cannot outsource this responsibility.

Sven Bluemmel
Victorian Information Commissioner

10 March 2021

[1] XYZ is a pseudonym. From 13 March 2021, it replaced a different pseudonym that appeared in an earlier version of the report. This was changed to remove a possible association with the another individual who was not involved in the circumstances described in the report.

Summary and recommendations

1. The Department of Health and Human Services (**DHHS**) is a Victorian government department that delivers policies, programs and services to support and enhance the health and wellbeing of Victorians.[2]

2. Finding Solutions is a program funded by DHHS to provide counselling and support to young people and their families.[3] DHHS funds numerous organisations (**funded agencies**) to deliver Finding Solutions and other programs. To assist funded agencies to deliver various DHHS programs, DHHS created and maintains the Client Relationship Information System for Service Providers (**CRISSP**). CRISSP is a client information and case management system that records client information, assists case management and enables reporting.[4]

3. In 2008, a contracted service provider (**CSP**) entered into a services agreement with DHHS to deliver part of the Finding Solutions program. The CSP was required to use CRISSP to record interactions with clients of the Finding Solutions Program.

4. Between September 2017 to October 2018 a former employee of the CSP ('**XYZ**') allegedly accessed information about clients on CRISSP without authorisation, after having left employment at the CSP (**data breach**). In October 2018, both the CSP and DHHS identified that XYZ had accessed CRISSP without authority and terminated the employee's access to the system. The alleged unauthorised access was also referred to Victoria Police.[5]

5. On 18 December 2018, DHHS notified the Office of the Victorian Information Commissioner (**OVIC**) of the data breach. OVIC and DHHS liaised about the data breach while DHHS investigated the incident internally and notified affected individuals.

6. On 25 February 2019, the Privacy and Data Protection Deputy Commissioner (**Deputy Commissioner**) commenced an investigation under section 8C(2)(e) of the *Privacy and Data Protection Act 2014* (**PDP Act**) for the purpose of deciding whether to issue a compliance notice under section 78 of the PDP Act. The investigation considered whether the CSP and DHHS took reasonable steps to protect personal information held in CRISSP as required by Information Privacy Principle (**IPP**) 4.1. The investigation considered steps taken by the CSP and DHHS to ensure that only the right people could access information in CRISSP.

7. Based on information gathered during the investigation, the Deputy Commissioner considered that the data breach had two main causes. The first cause was a failure by XYZ's supervisor to initiate the process to terminate XYZ's access to CRISSP when he no longer needed access to the system. This failure could be described as human error because it was contrary to the CSP's processes for deprovisioning access to CRISSP. This failure was due to an inadequate handover when one manager departed the role and another took over. The second cause was the absence of any effective secondary procedure or system for when the

[2] State Government of Victoria, 'Departments', www.vic.gov.au/departments.
[3] Victorian Department of Health and Human Services, *Finding Solutions program guidelines* (2012), available online at https://providers.dhhs.vic.gov.au/finding-solutions-program-guidelines-word ('Finding Solutions program guidelines').
[4] Finding Solutions program guidelines, 10.
[5] XYZ was also subject to a separate investigation into an alleged child sex offence. There is nothing before OVIC that indicates that the victim of that offence was a client of the CSP, or that XYZ successfully retrieved information about the victim from the CRISSP system.

primary mechanism for terminating a user's access to CRISSP failed. Neither DHHS nor the CSP had an effective secondary procedure or system in place.

8. With respect to the CSP, the Deputy Commissioner considered that it would have been reasonable for the CSP to implement a process or system that ensured a user's access to CRISSP was terminated in the event that the primary process to cease access was not followed. The Deputy Commissioner considered that this expectation would be reasonable given the nature of the information the CSP was responsible for in CRISSP and the potential risk of harm if that information were inappropriately accessed. Human error is a foreseeable risk, particularly the human error in this case. The Deputy Commissioner considers that the CSP did not sufficiently address this risk. The Deputy Commissioner found that a secondary checking process or system was a reasonable step the CSP should have taken to protect personal information stored in CRISSP. The absence of any secondary process or system was a breach of IPP 4.1 by the CSP.

9. With respect to DHHS, the Deputy Commissioner noted that DHHS primarily relied on its funded agencies to ensure correct user access to CRISSP. It contractually required the CSP to ensure user lists were up to date. However, the Deputy Commissioner found that DHHS held the information in CRISSP, so was obliged to protect it in accordance with IPP 4.1. The Deputy Commissioner examined the various steps that DHHS took to ensure that only the right people could access CRISSP, including system controls, contractual measures, and assurance processes. The Deputy Commissioner found that DHHS did not do enough to both support the CSP and to seek assurance that the CSP kept user access lists for CRISSP up to date. The Deputy Commissioner considered that regular monitoring of the ways in which the CSP was meeting its privacy and security obligations was a reasonable step expected to be taken by DHHS to protect the information in CRISSP. Although the initial contract for Finding Solutions was signed with the CSP in 2008, DHHS had never conducted an audit or other assurance activity under its services agreement with the CSP until the data breach occurred. As the Deputy Commissioner found no indication that DHHS regularly and appropriately monitored the privacy and security obligations of the CSP, the Deputy Commissioner finds that DHHS contravened IPP 4.1.

10. The Deputy Commissioner made the following recommendations to DHHS and the CSP:

    - **Recommendation 1:** That the CSP conduct regular checks of CRISSP user access lists (and the user access lists of other information systems) against payroll and other staffing records, at least once every three months.
    - **Recommendation 2:** That the CSP provide training of its staff about its privacy and security policies and procedures by 30 September 2020. The training should also aim to improve the general information security awareness of the CSP's staff. The training should be conducted at least once every two years.
    - **Recommendation 3:** That DHHS implement a risk-tiering framework for managing contracted service providers, and provide updates to the Deputy Commissioner on the progress of its implementation on 30 September 2020 and 31 March 2021.
    - **Recommendation 4:** That DHHS update and simplify the contractual framework and its guidance material for CRISSP and provide updates to the Deputy Commissioner on its progress towards meeting this recommendation on 30 September 2020 and 31 March 2021.

- **Recommendation 5:** That DHHS develop training that is specifically directed at the security and privacy obligations of systems administrators and Organisation Authorities and provide details of this training to the Deputy Commissioner by 31 March 2021.
- **Recommendation 6:** That DHHS implement a procedure to periodically check the currency of user lists for CRISSP and provide details of this procedure to the Deputy Commissioner by 30 September 2020.

(14 May 2020)

OVIC investigation

11. OVIC was notified of the data breach by DHHS on 18 December 2018 and 7 January 2019.

12. Under section 8C(2)(e) of the PDP Act, the Deputy Commissioner can carry out investigations 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 there was a serious, flagrant or repeated breach 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.

13. An investigation may also lead to the publication of a report and recommendations under section 111 of the PDP Act. Section 111 permits the Information Commissioner (**Commissioner**) to publish a report where the Commissioner considers it is in the public interest to do so. The Commissioner may report any act or practice the Commissioner considers to be an interference with privacy, or report about any matter generally relating to the Commissioner's function under the PDP Act.

14. DHHS is an 'organisation' for the purpose of Part 3 (Information Privacy) of the PDP Act, as a public service body within the meaning of the *Public Administration Act 2004*.[6]

15. The CSP, in relation to its provision of services associated with the Finding Solutions program, 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.[7]

16. The Deputy Commissioner considered the unauthorised access to CRISSP by XYZ presented a risk to the people whose information was stored on CRISSP, and that the unauthorised access might point to a serious contravention of the IPPs by the CSP or DHHS, or both.

17. On 25 February 2019, the Deputy Commissioner wrote to both the CSP and DHHS to advise that she intended to investigate the data breach under section 8C(2)(e) of the PDP Act.

Scope of investigation

18. Section 20 of the PDP Act says an organisation must not do an act, or engage in a practice, that contravenes an IPP as set out in Schedule 1 of the PDP Act. The Deputy Commissioner's investigation considered whether IPP 4.1 had been contravened by DHHS or the CSP. IPP 4.1 provides that:

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

19. Given the circumstances of the data breach, the Deputy Commissioner's investigation focussed on the steps taken by the CSP and DHHS to ensure that only the right users had access to CRISSP at the right times. In particular, the investigation considered:

    - the CSP's processes for providing and revoking access to CRISSP;

[6] PDP Act s 13(1)(c).
[7] PDP Act s 13(1)(j).

- steps taken by DHHS to monitor access to CRISSP by staff of funded agencies; and
- steps taken by DHHS to ensure the adequacy of the CSP's information security practices, particularly as they related to revoking system access.

Information considered

20. Both the CSP and DHHS cooperated with the Deputy Commissioner's investigation and provided substantial assistance to OVIC. Both organisations demonstrated a willingness to respond constructively to the Deputy Commissioner's investigation.

21. The Deputy Commissioner considered a range of information to reach the view outlined in this report including:

- written submissions from the CSP and DHHS;
- contracts and agreements between the CSP and DHHS with respect to the CSP's role as a funded agency;
- information gathered in meetings with representatives from the CSP and DHHS;
- various policies and procedural documents of the CSP and DHHS;
- training material provided by DHHS to the CSP as well as training material made available by DHHS to all funded agencies using CRISSP;
- system-generated reports detailing unauthorised access to the CRISSP system; and
- demonstrations of the CRISSP system and screenshots from CRISSP.

Background to the data breach

22. This section of the report describes the Deputy Commissioner's understanding of the relationship between DHHS and the CSP, and how the data breach occurred. It is based on the information listed at paragraph [21] above.

23. In 2008, the CSP entered into a services agreement with DHHS to deliver the Finding Solutions Program on behalf of DHHS. As part of its role in implementing Finding Solutions, the CSP was required to use CRISSP.

24. XYZ was employed by the CSP from 18 April 2016 to 13 September 2017.

25. After ceasing employment with the CSP, XYZ continued to access CRISSP without authorisation to find information about individuals recorded in CRISSP. This unauthorised access took place between September 2017 and October 2018.

26. In October 2018, the Department of Justice and Regulation (**DJR**) identified that XYZ had used CRISSP to view information about current and former clients of the CSP. Around the same time, the CSP and DHHS were also notified of XYZ's suspected unauthorised use of CRISSP by a staff member at the CSP – XYZ's former employer.

27. Upon being notified, DHHS and the CSP both terminated XYZ's access to CRISSP. DHHS also checked the access logs of CRISSP. That check revealed that XYZ had accessed CRISSP without authorisation 260 times between 13 September 2017 and 6 October 2018 involving 27 clients of the CSP.

28. On 18 December 2018, DHHS notified OVIC of the data breach.[8]

29. Victoria Police were separately notified of the data breach. At the date of this report, criminal proceedings not directly related to the data breach involving XYZ are ongoing.

Finding Solutions program

30. Finding Solutions provides case management and case work using mediation approaches with young people and their families. Case management includes case planning, coordination of services and referrals to other support services as required. Case work involves individual or family counselling and support for the young person and their family.[9]

31. The objective of Finding Solutions is to provide a rapid response to young people and their families in order to prevent family breakdown and entry into child protection and out-of-home care programs and systems.[10]

32. Finding Solutions is a Victoria wide program. The CSP is one of approximately 14 funded agencies operating the Finding Solutions program in Victoria.[11]

[8] This notification was made via telephone call to OVIC. Written notification of the incident was received by OVIC on 7 January 2019.
[9] Activity description (Human Services) Finding Solutions 31425.
[10] Finding Solutions Program Guidelines.
[11] Finding Solutions Program Guidelines.

CRISSP

33. CRISSP is a client information and case management system developed and administered by DHHS for use by registered funded agencies. Funded agencies use CRISSP as a case management tool with respect to the clients of the DHHS program they are funded to administer.[12]

34. CRISSP provides a range of functions for recording client information, assisting case management and enabling electronic reporting of data. Approximately 200 agencies and 1400 individuals are registered to use CRISSP.[13]

35. CRISSP records information (including personal, and in some cases sensitive, information) about people receiving certain DHHS services including:

    - name and date of birth;
    - address;
    - demographic information (ethnicity, indigenous status, country of birth, and language spoken at home);
    - relationships (including professional relationships);
    - placement address (if applicable);
    - alerts such as client risks or worker safety alerts;
    - case management records such as case notes, case plans and meetings;
    - any history of sexual abuse or exploitation;
    - services provision; and
    - allocated worker details.

Unauthorised access to CRISSP information

36. XYZ was employed with CSP as a case worker in the Finding Solutions program between April 2016 and September 2017. After September 2017, XYZ moved to a different role in which he was no longer working on Finding Solutions. Shortly after changing roles, XYZ ceased working at the CSP.

37. After ceasing employment at the CSP in 2017, XYZ's CRISSP access was not revoked until October 2018.

38. After ceasing employment at the CSP, XYZ was employed at another youth-focussed service provider (**youth service provider**), which is a funded agency managed by the one of the four divisions of DHHS. XYZ was employed as a lead tenant (a live-in mentor) and, as part of that role, was not required or authorised to access CRISSP.

[12] Letter from DHHS to OVIC, 14 March 2019.
[13] Letter from DHHS to OVIC, 14 March 2019.

39. In or around February 2018, after XYZ had ceased work at the CSP, a specialist unit of Victoria Police notified the East Division of DHHS that they had serious concerns about XYZ's access to vulnerable and at-risk children. Victoria Police told DHHS that the XYZ's work laptop had been handed into a police station and, while trying to locate the owner, officers had discovered child pornography on the laptop. The laptop had multiple user profiles and, as such, Victoria Police were unable to prove that the material was XYZ's.

40. DHHS notified the youth service provider of the allegation that XYZ may have accessed child pornography, and XYZ was stood down. DHHS did not discuss XYZ's CRISSP access with the youth service provider, as XYZ's role with this agency did not require it. Further, as XYZ was no longer an employee of the CSP (the CSP is managed by a separate division of DHHS to that managing the youth service provider), DHHS did not raise Victoria Police's concerns with the CSP.

41. In October 2018, a staff member employed by the DJR Youth Justice Program noticed that XYZ had accessed one of the Youth Justice Program's client files. Around the same time, an employee of CSP working in the Finding Solutions program also noticed XYZ's activity on CRISSP. The CSP and DJR notified DHHS of XYZ's suspected unauthorised access to CRISSP and, as a result, XYZ's access to CRISSP was revoked.

42. DHHS performed a check of the access logs on the CRISSP system with respect to XYZ's activity. The check found that, since ceasing employment with CSP, XYZ had accessed CRISSP 260 times involving 27 clients between 13 September 2017 and 6 October 2018. XYZ also conducted 150 searches of the CRISSP system. On each occasion, when XYZ accessed a file or conducted a search, personal information was displayed by the CRISSP system.

IPP 4.1

43. IPP 4.1 requires organisations to take reasonable steps to protect the personal information they hold from misuse and loss and from unauthorised access, modification or disclosure.

44. This section considers whether either DHHS or the CSP failed to take reasonable steps to protect personal information in the CRISSP system, as required by IPP 4.1. It examines the security measures and controls put in place by DHHS and the CSP to protect the personal information held in the CRISSP system, in order to determine whether those controls satisfied the requirements of IPP 4.1.

45. Whether a particular security measure or control is required by IPP 4.1 depends on a range of factors. Organisations must select security measures and controls appropriate to their circumstances and the risks they manage. Security measures and controls must also be proportionate to the potential harm that may result from a failure to protect the information. Factors relevant to assessing whether a particular step is reasonable include:

    - the type and amount of information held;
    - the potential impact of a privacy breach (on the people the information is about);
    - the likelihood of a breach occurring; and
    - the nature of the organisation and the difficulty (or cost) of implementing the step.[14]

46. In order to comply with IPP 4.1 an organisation should consider the foreseeable security risks to the personal information that they hold, then take reasonable precautions to mitigate those risks.

What personal information is CSP and DHHS required to protect?

47. IPP 4.1 requires organisations to protect personal information they hold.

48. Personal information is defined in section 3 of the PDP Act to mean:

> *information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.*

49. The sort of information held in CRISSP with respect to the Finding Solutions program is described above at paragraph [35]. It clearly includes personal information - that is, information and opinions about named individuals who are receiving services under the Finding Solutions program. Some of the information is also 'sensitive information' as defined in Schedule 1 of the PDP Act. Sensitive information is a subset of personal information that is afforded additional protections by the IPPs and includes, for example, information about sexual preferences or practices, and criminal record information.

50. Section 4(1) of the PDP Act explains the meaning of the word 'hold':

> *For the purpose of this Act, an organisation holds personal information if the information is contained in a document that is in the possession or under the control of the organisation,*

[14] Commissioner for Privacy and Data Protection, 'Guidelines to protecting the security of personal information: 'Reasonable steps' under Information Privacy Principle 4.1' (January 2017), pp 14–15. See also OVIC, *Guidelines to Information Privacy Principles* 'IPP 4: Data Security' (2019.B).

whether alone or jointly with other persons or bodies, irrespective of where the document is situated, whether in or outside Victoria.

51. As discussed above, the information accessed during the data breach was stored in CRISSP. The way DHHS and the CSP operate and access CRISSP is governed by three agreements that incorporate policies and manuals. The three agreements between DHHS and the CSP are:

    a. The Services Agreement dated 30 June 2015 (**Services Agreement**);[15]

    b. The Agreement for the access to and use of information on the CRIS and CRISSP systems dated 9 April 2008 (**CRISSP Agreement**);[16] and

    c. The eBusiness Access Agreement for Organisations between undated (**eBusiness Agreement**) which is also schedule 4 to the CRISSP Agreement.[17]

52. The Services Agreement deals with the services that the CSP provides DHHS including services that require the use of CRISSP. The Finding Solutions program is one of the services that the CSP provided to DHHS under the Services Agreement. The Services Agreement requires the CSP to comply with the PDP Act and the IPPs.

53. The CRISSP Agreement states that DHHS is responsible for 'maintaining and managing CRISSP'.[18] DHHS operates the system and acts as the system's administrator. DHHS has a right under the CRISSP Agreement to access information stored in CRISSP. The system is hosted on DHHS's behalf by CeniTex, the Victorian Government's central ICT support agency. For these reasons, the Deputy Commissioner considers that DHHS is in possession and control of all personal information stored in CRISSP. DHHS therefore holds that personal information and must protect it in accordance with IPP 4.1.

54. The CSP submits that:[19]

    it does not have possession or control of CRISSP information, or the information stored in CRISSP such that it 'holds' the personal information in accordance with section 4(1) of the PDP Act.

55. The CSP says that it only has access to CRISSP and the information contained in CRISSP. DHHS owns all rights in CRISSP and only grants the CSP a non-exclusive, non-transferable, royalty free licence for the term of CRISSP Agreement. Consequently, the CSP submits that it does not possess or control CRISSP or any personal information stored within CRISSP.

56. The Deputy Commissioner agrees with the CSP's submissions insofar as it extends to the 'possession' of information in CRISSP. However, the CSP can access, modify, and decide who (within its organisation) should and can have access to CRISSP information linked to client files the CSP is working on. Because of this, the Deputy Commissioner was satisfied that the CSP is in 'control' of the personal information stored within CRISSP relevant to its own

[15] State of Victoria as represented by the Department of Health & Human Services/Director of Housing Victoria and "CSP", 'Service Agreement aligned to the Victorian Common Funding Agreement, Agreement No 24273-15', 9 April 2008 (**Funding Agreement**)
[16] Department of Human Services and "CSP", 'Agreement for the access to and use of Information on the CRIS and CRISSP systems', 9 April 2008 (**CRISSP Agreement**).
[17] The Department of Human Services and "CSP", 'eBusiness Access Agreement for Organisations) publish date 17 December 2007' undated (**eBusiness Agreement**).
[18] CRISSP Agreement, clause 8.
[19] Letter from CSP to OVIC dated 22 November 2019

client's files. This includes the client files accessed during the data breach. The CSP therefore holds that personal information and must protect it in accordance with IPP 4.1.

57. The Deputy Commissioner found that both organisations 'hold' personal information that is stored in CRISSP. However, the reasonable steps that each organisation are required to take are different because of the varying degrees of possession or control they have over the CRISSP system and the information within it.

Protection of CRISSP information by the CSP

58. The CSP only has limited control over the personal information in CRISSP, as detailed above at paragraph [56]. However, it does play an important role in ensuring that only the correct users have access to CRISSP: it is primarily responsible for keeping its list of active CRISSP users up to date.[20]

59. The CSP described the steps it takes to protect the personal information it holds. The CSP said that it has robust physical security and computer security measures in place, along with protocols related to privacy protections for the communication of personal information. It also described the checks that it does on employees:

> *… [the CSP] has extensive pre-employment screening to ensure a prospective employee is suitable for employment and subsequently, to use databases such as CRISSP. This includes National and International Police Checks, Working with Children Checks, verifying professional registration, verifying qualifications, proof of identity, psychometric assessment and two reference checks prior to employment. Regular, ongoing compliance checks take place throughout the employee's employment.*[21]

60. Given that the data breach was caused by a failure to remove XYZ's access to CRISSP at the appropriate time, the Deputy Commissioner's inquiries focussed on the CSP's processes for provisioning and deprovisioning access to CRISSP.

61. In accordance with the CRISSP Agreement and eBusiness Agreement, the CSP's Organisation Authority (**OA**) was responsible for ensuring that only current employees with the correct authority had access to the CRISSP system.[22] An OA is a designated position which has certain responsibilities under the agreements that govern the CSP's access to CRISSP. To revoke a user's access to CRISSP, the OA is responsible for ensuring that a 'CRISSP Remove User Form' is sent to DHHS. DHHS then revokes the relevant user's access to CRISSP.[23] Under both the CRISSP Agreement and the eBusiness Agreement, the OA is responsible to:

    a. Verify that an employee's job or position within [the CSP] warrants them to have access to CRISSP;[24]

    b. Maintain the currency of the registered eBusiness Users for their organisation (for example, advice on de-registering User accounts);[25] and

[20] CRISSP Agreement, clause 16; eBusiness Agreement, schedule 2 Organisation Authority, item 2.
[21] Letter from CSP to OVIC, 15 March 2019, p 6.
[22] CRISSP Agreement, clause 16.6.
[23] CRISSP Agreement para 16.6(c), and Organisation Authority Processes Factsheet, published October 2017; eBusiness Agreement, schedule 2 Organisation Authority.
[24] CRISSP Agreement, clause 16.6; eBusiness Agreement, schedule 2 Organisation Authority, item 2.2.
[25] CRISSP Agreement, clause 16.6; eBusiness Agreement, schedule 2 Organisation Authority, item 2.4.

c. Ensure users' access rights are reviewed at regular intervals.[26]

At the time of the incident the OAs at the CSP were the managers of two CSP divisions. These two OAs were responsible for approving access to CRISSP for their respective divisional areas.

62. However, the OAs were not regular CRISSP users, and the CSP's procedure for the deactivation or revocation of a user's access was initiated by each user's direct supervisor, rather than the OA. The CSP described the process for deprovisioning access to the system as follows:

> *The responsibility for removing users from the system when they leave either the program or the organisation (or both), rests with the direct supervisor of the employee. The supervisor first deactivates the user on CRISSP, and then submits the form to DHHS to remove the user from the system.*[27]

63. At the time of the incident, there was a changeover of team leaders in XYZ's work unit. Because of this changeover, the revocation of XYZ's access to CRISSP was overlooked, as was the submission of the 'Remove User Form' to the CSP's OA, and subsequently DHHS. For this reason, XYZ's access privileges remained active.

Did the CSP take reasonable steps as required by IPP 4.1?

64. The Deputy Commissioner found that the CSP's procedure relied solely on the team leader initiating the offboarding process for CRISSP users, by first deactivating the user within CRISSP, and then completing a 'Remove User Form'. This created a single point of failure, meaning that where a team leader failed to deactivate a user and submit the relevant form, the user could retain access indefinitely. That occurred with respect to XYZ's access to the system, leading to the data breach.

65. The failure of the CSP's individual staff member to deactivate XYZ's access to CRISSP at the appropriate time could be described as 'human error'. However, the Deputy Commissioner also considered that the access and revocation model employed by the CSP, and described above, was a factor that contributed to the data breach.

66. The process for offboarding an employee at the CSP relied on supervisors following the correct offboarding process. There was no second line of defence or alternative process if the correct process was not followed. A range of processes could have been used to provide a secondary check to ensure users were appropriately deprovisioned, even if the primary mechanism failed. For example, the CSP could have:

- conducted regular checks of CRISSP user lists by team supervisors;
- conducted regular checks of CRISSP user lists against payroll or other records held by the CSP's human resources team; and
- developed an offboarding process which required HR, or someone other than the team supervisor, to confirm system accesses had been deprovisioned when staff moved jobs or left the organisation.

[26] CRISSP Agreement, clause 16.6; eBusiness Agreement, schedule 1 IT Security Policy, item 2.4; eBusiness Agreement, schedule 2 Organisation Authority, item 2.5.
[27] Letter from CSP to OVIC, 15 March 2019, p 4.

67. In considering whether implementing a secondary procedure such as those listed above is a reasonable step that is required by IPP 4.1, the Deputy Commissioner considered matters including:

    - the nature of the information held in CRISSP being both sensitive information as defined in the PDP Act, and information likely be regarded as being of a sensitive, or delicate, nature by the people it was about.
    - the potential consequences of failing to remove a user's access to CRISSP and allowing unauthorised access, given the nature of the information stored in CRISSP and the vulnerability of the people it is about; and
    - the ease with which a procedure could be implemented to account for the possibility of human error and provide a secondary deprovisioning process.

68. The Deputy Commissioner also considered the commitments made by the CSP in the CRISSP Agreement and eServices Agreement to keep its user lists up to date.[28] In considering these matters, the Deputy Commissioner found that implementing a secondary procedure for deprovisioning is a reasonable step that should have been considered under IPP 4.1 to protect personal information held. The CSP should not have relied solely on a single employee following the correct procedure to ensure that user access to CRISSP was ceased at the appropriate time. By not putting in place any procedure to account for the risk of human error in the deprovisioning process, the CSP did not protect the personal information in CRISSP as required by IPP 4.1.

69. It is therefore the Deputy Commissioner's view that the CSP contravened IPP 4.1 by not having any mechanism in place to account for the risk of human error in the deprovisioning process for CRISSP.

70. The Deputy Commissioner notes that the CSP has made significant improvements to its offboarding processes since the incident, which are detailed below at paragraphs [127] to [131].

Recommendations to the CSP

71. The Deputy Commissioner made the following recommendations to the CSP with respect to the contravention identified above:

    - **Recommendation 1:** That the CSP conduct regular checks of CRISSP user access lists (and the user access lists of other information systems) against payroll or other staffing records, at least once every three months.
    - **Recommendation 2:** That the CSP provide training of its staff about its privacy and security policies and procedures. The training should also aim to improve the general information security awareness of the CSP's staff. The training should be conducted at least once every two years.

72. When determining how often the above checks and training should take place, the Deputy Commissioner weighed up the nature of the information held in CRISSP and the potential consequences of failing to adequately protect that information with the ease with which the

[28] CRISSP Agreement, clause 16.6; eBusiness Agreement, schedule 2 Organisation Authority, item 2.

checks and training could be implemented without significantly impacting the day-to-day operations of the CSP.

Protection of CRISSP information by DHHS

73. When DHHS was asked how it ensured that CRISSP user accounts were provisioned and revoked appropriately, it submitted that:

> *The arrangements between each funded agency and the department is governed by a service agreement, which is largely on standard terms.*
>
> *Clause 17 and 19 of the department's standard service agreement deal with privacy. […] In essence, the service agreement places the onus on funded agencies to comply with all privacy law requirements.*
>
> *Services are required to certify compliance with a number of service agreement requirements on annual basis via a Service Agreement Compliance Certification (SACC). The SACC requires organisations to attest that their practices and systems for the collection, use, disclosure, protection, and disposal of personal information and health information are compliance with the PDP Act and the Health Records Act 2001 required under the service agreement.*
>
> *The department relies upon agencies to manage and validate CRISSP user access within their organisation. The OA function within each agency is critical to this process, as the OA has sufficient knowledge of, and access to, information on the structure and operation of their organisation to ensure CRISSP user access is reflective of their workforce on a real time basis.*
>
> *The department is able to conduct audits in response to identified concerns, as occurred with respect to this incident. However, the department relies on agencies to audit their own internal access controls for CRISSP due to the fact the department does not have access to agency employment records. Each agency OA is responsible for approving access on the organisations' behalf and auditing access accounts.*[29]

74. In essence, DHHS relies on funded agencies to both maintain the currency of user accounts to CRISSP, and to protect the information that those agencies access. DHHS does this by imposing contractual controls through the three agreements listed in paragraphs [51]. However, DHHS still retains control of the CRISSP system and possession of the information stored on it. As discussed at [47] to [57] above, it holds personal information in CRISSP and must take reasonable steps to protect that information.

75. The Deputy Commissioner is of the view that outsourcing parties should adopt a risk-based approach to protecting public sector information.[30] This requires them to balance the level of assurance and controls required to mitigate risk with the kinds of information involved and the possible consequences of a compromise to that information. The greater the likelihood and consequences of a compromise to the confidentiality, integrity, or availability of the information, the greater the effort expected from organisations to guard against that risk.[31]

---

[29] Letter from DHHS to OVIC, 14 March 2019, p 4.

[30] For a definition of public sector information please refer to the OVIC *Victorian Protective Data Security Standards – Glossary*. Available at https://ovic.vic.gov.au/resource/vpdss-glossary-of-protective-data-security-terms/

[31] For further information see: Commissioner for Privacy and Data Protection, *Guidelines for outsourcing in the Victorian public sector: Accompanying guide*, 12. Confidentiality, integrity, and availability, are concepts defined in OVIC *Victorian Protective Data Security Standards – Glossary.*

76. To consider whether DHHS's approach to protecting the information it held jointly with the CSP accorded with IPP 4.1, the Deputy Commissioner considered three aspects of DHHS's protection of this information with respect to provisioning and deprovisioning CRISSP users. The three aspects considered were:

    - **Technical controls**: Controls that DHHS built into the CRISSP system to ensure only the right CSP's users had access to the right information;
    - **Contractual controls**: Agreements between DHHS and the CSP designed to ensure that appropriate steps were taken to keep CRISSP user lists up to date; and
    - **Assurance and support**: Steps taken by DHHS to support the CSP in meeting its privacy and security obligations, and to assure itself that the CSP was meeting those obligations.

Technical controls

77. As outlined above, the CSP and DHHS both hold any case information stored in CRISSP relating to the work of the CSP. However, as the operator of the CRISSP system, DHHS is the only organisation that can implement technical and system controls within CRISSP itself. To ensure that only the right people could access the right information, DHHS implemented several controls within the CRISSP system, including:

    - segmented access and security profiles;
    - audit logs and monitoring; and
    - a system that automatically deactivated unused user accounts.

78. With respect to segmented access controls, each funded organisation that has access to CRISSP is set up with its own security profile by DHHS. This profile provides access to the information that is relevant to the program the funded organisation is responsible for administering. DHHS set up the Finding Solutions program as a 'stand-alone' profile, which means that other agencies (and employees of those agencies) are unable to access Finding Solutions program information on CRISSP.

79. With respect to audit logs, DHHS advised that a 'flag' is assigned to a client file whenever it is accessed. Users can view these flags via the client file. This allows CRISSP users (and, if necessary, DHHS) to check to see who has accessed their clients' files and to alert their supervisor if they believe a file is being accessed by an unauthorised person, or by a person breaching 'need to know' principles. These audit logs allowed DHHS to identify all records accessed by XYZ once it became aware of XYZ's unauthorised access.

80. With respect to the automated removal of inactive accounts, DHHS implemented an automatic check within the CRISSP system that identifies and disables inactive user accounts. At the time of time information breach, the CRISSP system was set up to identify accounts that had been inactive for 60 days. Users of these accounts were sent an email advising they have 14 days to take steps to retain their access to CRISSP. At the end of the 14 days, if the account remained inactive, the account would be deactivated. However, the check did not trigger for XYZ's account as they had not been inactive on the system for the required period – XYZ was still using CRISSP. The Deputy Commissioner was not satisfied that this control was an effective mechanism for preventing intentional inappropriate access to CRISSP.

81. Nonetheless, the Deputy Commissioner was satisfied that there were a range of other technical controls in place that allowed DHHS, working with its funded agencies, to manage individual user access.

Contractual controls

82. As noted above, DHHS primarily relies on funded agencies to maintain the currency of user accounts in CRISSP. The Deputy Commissioner considered the contractual controls that DHHS imposed on the CSP requiring them to maintain the currency of their user accounts in CRISSP.

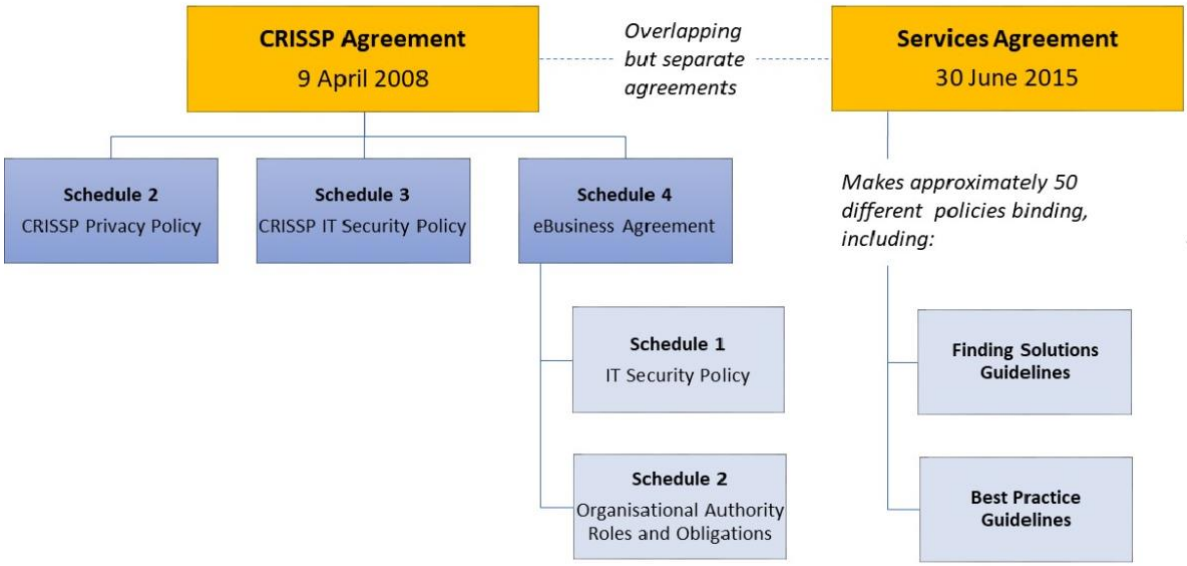
83. As noted in paragraph [51], there are three agreements between DHHS and the CSP that contractually require the CSP to maintain the currency of user accounts in CRISSP. The three agreements refer to policies and manuals that were regularly updated. These policies and manuals are given contractual weight insofar as a breach of these policies constitutes a breach of their parent agreement. More specifically the Services Agreement and CRISSP Agreement required the CSP to comply with the following policies:

    a. CRISSP Agreement – Schedule 2 Privacy Policy, Schedule 3 IT Policy, Schedule 4 Organisation Authority duties and the CRISSP Operations Manual.

    b. Services Agreement – Funding Solutions Guidelines, Youth Services Best Practice Guidelines and the CRISSP User Guide.

84. The Deputy Commissioner observes that the three agreements, policies and manuals create a complex, overlapping structure that is difficult to piece together and interpret. At a high level, the way the agreements interact is illustrated in Figure 1 below.

Figure 1: Relationship between agreements governing CRISSP usage by funded agencies



85. The obligations relating to security, audit, notification, and the contractual consequences for a privacy breach sit across the three agreements. The privacy obligations, as well as the requirements about provisioning and deprovisioning users, are replicated in parts across the three agreements and supporting documents. The policies and manuals also overlap and

replicate the operational processes involved in provisioning and deprovisioning access. Finally, many documents are outdated insofar as they refer to old legislation, or where one document is the replacement for another.

86. In reviewing the contractual controls, the Deputy Commissioner accepted that all three agreements were operative. The Deputy Commissioner considered the following categories of contractual controls in relation to provisioning and deprovisioning users:

    a. Clarity of obligations – Did the agreements make it clear whether DHHS or the CSP was responsible for provisioning and deprovisioning access when required?

    b. Effect of breaches – What would result if the CSP breached the PDP Act or IPPs?

    c. Notification of breaches – What was the CSP's responsibility to notify DHHS of any privacy breach?

    d. Audit of compliance – Was the CSP required to audit privacy compliance, or seek an external audit of privacy compliance?

Clarity of obligations

87. Under the CRISSP Agreement, DHHS is responsible for:[32]

- maintaining and managing CRISSP;
- maintaining the DHHS e-Business domain;
- organising the provision of an appropriate level of helpdesk and user support for both technical and business purposes;
- providing once-off initial training to CSP staff, and thereafter to maintain and update online training tools; and
- providing registration of all users submitted through the CSP's nominated OA.

88. Under the CRISSP Agreement and eBusiness Agreement, the CSP is responsible for:

- supporting users through agreed practices for privacy, security and access to CRISSP outlined in the CRISSP Agreement;
- establishing an Organisational Authority as per details stated in Schedule 4 of the CRISSP Agreement; and
- complying with Schedule 2 – CRISSP Privacy Policy, Schedule 3 – CRISSP IT Security Policy, and Schedule 4 – Organisation Authority.[33]

89. Clause 13 of the CRISSP Agreement states that:

> *[DHHS] will provide training during the initial implementation of CRISSP to Organisation employees. Ongoing user training is the responsibility of the Organisation. [DHHS] will provide electronic training guides and updates.*

[32] CRISSP Agreement, para 8.

[33] CRISSP Agreement at clause 9, pg 12. Please note that this report only includes the relevant obligations and does not list all of DHHS's obligation set out at clause 9.

90. Clause 16 of the CRISSP Agreement and Item 2 of the eBusiness Agreement says the responsibilities of the Organisation Authority (an employee of the CSP) include:

- maintaining the currency of the CSP's structure details for the CSP (for example adding, removing or changing the CSP's address details);
- maintaining the currency of the registered e-business Users for the CSP (for example advice on de-registering User accounts); and
- ensuring that users' access rights are reviewed at regular intervals.

91. While concerned that the contractual documents are complex and difficult to piece together, the Deputy Commissioner is satisfied that the three agreements contained provisions showing that it was the CSP's responsibility to ensure that only appropriate users had access to CRISSP.

Relevant obligations to protect privacy and consequences of breach

92. At a high level, the CRISSP Agreement and Services Agreement contain clauses requiring the CSP to adhere to the *Privacy Act 2000* (Vic) (as it was prior to 2014, and the introduction of the PDP Act), and specifically that the CSP agrees to 'carry out and discharge the obligations contained in the IPPs as if it were [DHHS] under the [*Privacy Act 2000*].'[34] In addition, each of the three agreements contain specific obligations about provisioning and deprovisioning access to CRISSP as outlined above.

93. None of the three agreements explicitly set out any consequences for a breach of privacy obligations.

94. Nevertheless, in respect of the CRISSP Agreement and eBusiness Agreement, a breach of the OA's obligations, including about provisioning or deprovisioning access, may constitute a breach of a material term. Clause 5.3 of the CRISSP Agreement states that:

> *[A]n Organisation's access to CRISSP is governed by the rules set out in the Operations Manual. The Organisation agrees to comply with these access rules. For the avoidance of doubt, a failure by the Organisation to comply with these access rules will be deemed to be a material breach of this Agreement.*[35]

95. Clause 2.4 of the CRISSP Agreement provides that a material privacy breach could result in the CRISSP Agreement being terminated if that privacy breach is not rectified within 14 days of written notice. If the CRISPP Agreement was terminated, it would result in the CSP losing access to the CRISSP system and thus being unable to perform some services in the Services Agreement. On balance, this is not a strong privacy contractual control. The consequences for a material privacy breach is termination without any steps or penalties in between. This, in turn, would likely lead to the Services Agreement either being significantly reduced in scope or terminated.

96. On the other hand, in respect of the Services Agreement, a breach of privacy obligations allows DHHS to either suspend or cease particular services. In cases of a material breach, or an unremedied breach, a breach of privacy obligations could also result in termination of the Services Agreement.

[34] CRISSP Agreement, para 6.1(c).
[35] CRISSP Agreement, para 5.3.

97. A strong privacy contractual control in a commercial agreement would link breaches of privacy to abatements or penalty payments. This type of control leverages the commercial pressure on the contractor. Nevertheless, that type of control is not without its disadvantage, particularly given the type of services provided by the CSP under the Services Agreement.

Notification

98. Clause 17 of the Services Agreement requires the CSP to notify DHHS where the CSP 'becomes aware of a breach, or possible breach' of any of the CSP's obligations under the PDP Act.[36] While clause 17 does not explicitly set out the consequence of failing to comply with this obligation, a failure to notify would at least be a breach of the Services Agreement.

Assurance and audit activities

99. The CRISSP agreement states that CRISSP will be monitored by DHHS to detect any unauthorised access attempts, multiple unsuccessful logons, and inactive user accounts.[37] The Services Agreement permits DHHS to conduct audit and performance reviews.[38]

100. A strong audit clause would require to the CSP to either audit its CRISSP users' access or have an independent third-party audit that use. The Services Agreement is of significant value and relates to a system that holds information of a sensitive nature. It would be reasonable for the contract to include a strong audit clause requiring the CSP to conduct a periodic internal or external audit of CRISSP user controls, and a frequent internal check on authorised users and their activities.

Contractual controls – conclusion

101. On balance, the Deputy Commissioner found there were contractual controls in place between the parties and that, together, the CRISSP Agreement and the Services Agreement:

- outline the obligations of the parties;
- contain notification clauses;
- set out the parties' obligations under the *Privacy Act 2000* (which are largely similar to those in the PDP Act);
- provide DHHS with an ability to monitor the CSP's compliance with privacy and security standards; and
- include consequences for breaches.

102. Although the Deputy Commissioner considered that, overall, a contractual framework was present, the Deputy Commissioner considered that there were several areas in the contractual framework that could be improved. These included:

- the clarity of the CSP's obligations. The agreement between the CSP and DHHS relating to CRISSP was contained in a large number of overlapping agreements, policies, and manuals;

[36] Services Agreement, para 17.2(f).
[37] CRISSP agreement, para 4.1 of schedule 2.
[38] Services Agreement, clause 9.1.

- the addition of more explicit consequences for privacy breaches, including abatements or other penalties that could be utilised as an alternative to terminating an entire agreement; and
- a stronger audit clause that would require the CSP to either audit its CRISSP users' access, or to have an independent third-party audit that access.

Support and assurance

103. Clause 9.1 of the Services Agreement sets out that DHHS may conduct, or engage a third party to conduct, audits in certain circumstances. Schedule 2 of the CRISSP Agreement states that CRISSP will be monitored by DHHS to detect any unauthorised access attempts, multiple unsuccessful logons, and inactive system users.

104. The outsourcing guidelines issued by the former Commissioner for Privacy and Data Protection indicate that ongoing support and assurance is an essential part of protecting information held by contractors:

> *… an outsourcing party will have an ongoing responsibility for the official information held by its [Contracted Service Providers] and must continue to ensure that data security and privacy obligations are met during the life of the State contract.*
>
> *In order to do this effectively, outsourcing parties should work collaboratively with their [Contracted Service Providers] to actively identify and mitigate privacy and security risks throughout the life of the arrangement. …*
>
> *This means that outsourcing arrangements can't just be 'set and forget' exercises. Outsourcing parties should make sure they have appropriate measures in place to ensure that they, and their [Contracted Service Providers], are meeting their obligations under the VPDSF and the IPPs.*
>
> *Outsourcing parties should subject the acts and practices of their [Contracted Service Providers] to at least the same level of ongoing scrutiny in relation to privacy and data security as they would their internal acts or practices.*
>
> *This may mean:*
>
> - *regular surveys, reports, site visits and/or audits are conducted on how the [Contracted Service Providers] is handling official information*
> - *regular reviews of the outsourcing arrangement as a whole from a privacy and data security perspective, including regular re-assessment of risks and associated mitigation strategies*
> - *responding to requests for assistance or advice from their [Contracted Service Providers] about their privacy and data security obligations and working with [Contracted Service Providers] to respond to data breaches and/or manage security incidents.*[39]

105. As detailed at [73] funded agencies are required to certify to DHHS that they are complying with the services agreements on an annual basis. Funded agencies do this by signing a Service Agreement Compliance Certification (**SACC**). The SACC requires the funded agency to attest that their practices and systems for the collection, use, disclosure, protection, and disposal of personal information are compliant with the PDP Act required under the services agreement. However, in meetings with OVIC, DHHS staff noted that this can be a 'check box'

[39] Commissioner for Privacy and Data Protection, *Guidelines for outsourcing in the Victorian public sector: Accompanying guide*, 30.

process and not provide a high degree of assurance that agencies are meeting their privacy and security obligations.

106. As detailed above at [82] to [102], the Services Agreement and CRISSP Agreement allow DHHS to conduct audits and compliance checks to ensure that the CSP is meeting its privacy, security, and other obligations. The CRISSP Agreement also specifies that checks will be conducted by DHHS on CRISSP access logs to identify unsuccessful logins or unauthorised access attempts.[40]

107. However, DHHS told OVIC that between 2008 (when the CSP began work on Finding Solutions) and the time of the data breach, DHHS had not proactively performed an audit or compliance check on the CSP regarding its privacy or security obligations. DHHS also did not check CRISSP access logs until it became aware of the data breach.

108. DHHS has previously received recommendations about oversight of funded agencies.[41] In discussing its approach to managing the CSP contract with OVIC, DHHS acknowledged those recommendations. It said that it had been developing a more active approach to contract management. DHHS demonstrated to the Deputy Commissioner's satisfaction that it has an extensive program of work underway which will allow it to more actively audit funded agencies, based on risk-assessments of those agencies. DHHS says the risk-tiering framework it has established as part of this program of work will operate as a means of identifying agencies that may pose a risk to DHHS in terms of client safety, services not being provided, or issues for governance and administration, including information security. At the time of the data breach, the risk-tiering framework was not in place. However, DHHS informed OVIC that it began its implementation of the proposed framework on 1 July 2019.[42]

109. OVIC also sought to understand how DHHS supported the CSP to allow it to adhere to its security and privacy obligations under the Services Agreement and CRISSP Agreement. DHHS carried out a range of activities to support the CSP (and other CRISSP users), including:

- developing user guides and other documentation for CRISSP users;
- providing training. Over the life of the Services Agreement, DHHS advised that it delivered 13 training sessions for the CSP about CRISSP; and
- staffing a help desk to answer questions from users of CRISSP and other departmental information systems.

110. However, the material produced by the department is lengthy and was in some regards unclear. The CSP told OVIC:

> *The CRISSP User Guide October 2011 consists of 26 separate .pdf documents each of approximately 1 – 8 pages. The 'IT Support for CRISSP' document requires that […] 'Existing users who leave an organisation must have their access revoked as soon as possible […]. Removing a user for CRISSP (and CRIS) is done by completing the "CRISSP Remove User Form" on the CRISSP Website […].*

[40] CRISSP Agreement, Schedule 2 – CRISSP Privacy Policy para 4.1, 21.
[41] Victorian Auditor General's Office, 'Contract Management Capability in DHHS: Service Agreements' (September 2018); Commissioner for Privacy and Data Protection, 'Review of Information Governance Arrangements in the Department of Health and Human Services (DHHS)' (January 2017).
[42] Letter from DHHS to OVIC, 6 February 2020

> *However, none of the Best Practice Guidelines, CRISSP User Guide nor 'Remove User Form' make clear which entity (DHHS, the community service provider or end user) have the obligation to remove the end user's access.*[43]

111. The CSP also noted that the DHHS did not provide training for administrators and managers about their special responsibilities in overseeing CRISSP usage:[44]

> *During the onboarding process, employees are given the CRISSP user guides and given one on one training by a co-worker or Team Leader in how to use the database. They are also booked in for the next available training via DHHS through the CRISSP web page. Currently there is no specific training for Team Leaders or managers that highlights their responsibilities in managing access. We think that would be of benefit.*

112. OVIC observed that the CRISSP user manuals and documentation were unclear about how a funded agency should check its active users to ensure user access lists were up to date. In early discussions between OVIC and the CSP, the CSP said it was unable to access a list of active users within CRISSP, and as such it relied on DHHS to provide user lists. When OVIC first asked DHHS to confirm this was the case, it said:

> *There is no function that allows an Organisation Authority to view a list of their agency's active CRISSP users. An Organisation Authority would need to make a request to the eBusiness [team in DHHS] to acquire such a list.*

113. Later, during a demonstration of CRISSP, a DHHS specialist staff member was able to show OVIC how a list of CRISSP users could be accessed by staff of the CSP. As part of the investigation OVIC contacted the CSP to confirm that it had access to the function that allows it to view the list of current CRISSP users, and if it was aware of how to use the function. The CSP confirmed that although it did have access to the administration function, until OVIC raised the issue of self-auditing, it had not been told how to utilise the function. Further, the CSP advised that as part of its response to the incident it had repeatedly asked the DHHS CRISSP help desk to provide it with current lists of CRISSP users. The CRISSP help desk did not inform the CSP of the administration function contained within CRISSP that would allow it to self-audit without having to request lists of users from DHHS.

114. While it is appropriate that the CSP can access a list of its current users, the confusion around this issue highlights a lack of clarity within the training and manuals provided by DHHS to its contracted service providers about how they can manage access privileges.

115. The Deputy Commissioner was also concerned about the lack of any compliance checks over the life of the CRISSP agreement. The Deputy Commissioner also considered that simpler guidance could have been provided to the CSP to assist it in meeting its obligations to onboard and offboard users from CRISSP.

Did DHHS take reasonable steps as required by IPP 4.1?

116. DHHS relies on funded agencies to manage and validate CRISSP user access. It needs to do so because of the large number of agencies that it funds (approximately 1600). For DHHS to operate effectively in such an outsourced model of delivery, it outsources some of its privacy and security responsibilities to the funded agencies that hold information on its behalf.

[43] Letter from CSP to OVIC, 15 March 2019, 2.
[44] Letter from CSP to OVIC, 15 March 2019, 5.

117. However, given DHHS still holds the information used by its funded agencies that is stored in systems such as CRISSP, it must protect that information. In considering the extent of the reasonable steps that DHHS needs to take to protect this information, the Deputy Commissioner considered the matters outlined above at paragraph [67].

118. DHHS is a large organisation that delivers projects in housing, disability, family and child services and programs, public health services, public hospitals, health, mental health and aged care services, the prevention of family violence and violence against women, and sport and recreation supporting the community in metropolitan, rural and regional Victoria. DHHS has over 10,000 employees to manage and works with 1600 funded agencies that carry out various activities on its behalf.[45] This delivery model means there is a limit to the extent to which it can monitor all its funded agencies.

119. The Deputy Commissioner recognises that managing such a wide variety of programs and many funded agencies is complex. However, the Deputy Commissioner considers that it is insufficient to rely exclusively on contract without providing assurance and support proportionate to the privacy and security risks related to each provider.

120. The Deputy Commissioner considered that, at the time of the incident, DHHS's support and assurance processes with respect to the CSP were inadequate. In particular, the Deputy Commissioner observes that from 2008 until the data breach, DHHS had not performed an audit or compliance check of the proper use of CRISSP by the CSP. The Deputy Commissioner was also concerned that DHHS had taken no steps, as the administrator of the CRISSP system, to verify the currency of CRISSP user lists.

121. It is therefore the Deputy Commissioner's view that DHHS contravened IPP 4.1 by:

- failing to conduct any privacy or security checks on the CSP between 2008 and 2018; and
- failing to take steps to confirm the currency of the CRISSP user list between 2008 and 2018;

122. The Deputy Commissioner also considered that DHHS could have provided better support to the CSP to assist it in meeting its privacy and security obligations. However, the Deputy Commissioner was not satisfied that this lack of support was a breach of IPP 4.1.

Recommendations to DHHS

123. The Deputy Commissioner made the following recommendations with respect to these matters:

- **Recommendation 3:** That DHHS implement a risk-tiering framework for managing contracted service providers and provide updates to the Deputy Commissioner on the progress of its implementation on 30 September 2020 and 31 March 2021 (noting that DHHS began its implementation of such risk-tiering framework on 1 July 2019).
- **Recommendation 4:** That DHHS update and simplify the contractual framework and its guidance material for CRISSP and provide updates to the Deputy Commissioner on its progress towards meeting this recommendation on 30 September 2020 and 31 March 2021.

[45] Department of Health and Human Services, *Annual Report 2017-18*, published in September 2018.

- **Recommendation 5**: That DHHS develop training that is specifically directed at the security and privacy obligations of systems administrators and OAs and provide details of this training to the Deputy Commissioner by 31 March 2021.
- **Recommendation 6:** That DHHS implement a procedure to periodically check the currency of user lists for CRISSP and provide details of this procedure to the Deputy Commissioner by 30 September 2020.

Whether to issue a compliance notice

124. A compliance notice may be issued by the Deputy Commissioner in response to a serious, flagrant or repeated breach 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. This section of the report discusses matters relevant to that decision, including changes to DHHS and CSP practices that have occurred since the data breach.

125. For a compliance notice to be issued, the Deputy Commissioner must be satisfied that:

- a serious, repeated, or flagrant contravention of the IPPs has occurred; and
- in the circumstances, it is appropriate for the Deputy Commissioner to exercise her discretion to issue a compliance notice in response to the contravention.

126. The response of DHHS and the CSP to the data breach is relevant to both these matters. Both DHHS and the CSP have responded to this incident in a manner that reflects its seriousness.

The CSP response to the data breach

127. Immediately after the data breach the CSP amended its online privacy module training. The CSP spoke to all of its employees about the systems each person used and reiterated how important the deactivation of users is in ensuring privacy.

128. The CSP advised that the following changes have been made to its internal CRISSP activation and deactivation processes:

- with respect to employment changes within the CSP (where an employee moves from a program that requires CRISSP to one that doesn't) the current manager will be required to indicate on an 'employment change form' that CRISSP access has been revoked. The 'employment change form' is required to be sent to Human Resources for final sign off.
- with respect to employee offboarding, the current manager will be required to indicate on a 'cessation checklist' that CRISSP access has been revoked. This form is also sent to Human Resources for final sign off.
- if either of the above forms do not indicate that CRISSP access has been revoked, the Human Resources Administrator will follow up the manager to ensure that it has been revoked.[46]

129. In addition to the above changes, the CSP have created a CRISSP Database access policy which requires a six-monthly audit of the CRISSP system by Human Resources and Senior Management to ensure that only current employees who require access to CRISSP have access.

130. The CSP has provided OVIC with a copy of draft policies and procedures that give effect to these changes.

131. The CSP has also engaged two external consultants to review and provide advice on:

    a. its privacy policy;

[46] Letter from CSP to OVIC, 15 March 2019.

b. its security and data policy;

c. its provisioning and deprovisioning processes; and

d. any potential risks associated with the above.

DHHS response to the data breach

132. DHHS advised that it has made or is in the process of making several changes to the management of funded agency contracts, and CRISSP access, including:

- Introducing a risk tiering framework, which will be used to rank the risk of each of the DHHS funded agencies. The new risk-based framework will consider the range and complexity of agencies, service types and service complexities. Specifically, the framework will focus on:
    - a risk tiering guide to the oversight of funded agencies;
    - monitoring activities (including Desktop reviews and Service Agreement Compliance Certification)
    - performance escalation framework; and
    - performance reviews and action plans.

  This approach will operate as a means of identifying agencies that may pose a risk to DHHS and will allow for the risk indicators to be documented as well as provide a consistent approach to identifying risk and ensuring compliance. By adopting a risk-based framework to contract management, DHHS will be able to build proportionality into the compliance requirements associated with each Service Agreement.

- Introducing a performance escalation framework which will be developed to encourage a consistent approach to performance management. This framework will include:
    - how to classify performance issues;
    - how to respond to these issues;
    - when issues should be escalated; and
    - where they should be escalated to.
- Implementing a quarterly compliance regime that requires funded agencies to audit their CRISSP users. This will be done by providing the agencies with a list of their current registered CRISSP users. Each agency must confirm, by completing a declaration form, that each individual on the CRISSP user list is a current employee who requires CRISSP access. Any ex-employees on the CRISSP user list, or employees whose job no longer requires CRISSP access, must be removed by completing and returning either the Remove User or User Update form to DHHS; and
- In addition to the quarterly review process, developing a self-service report functionality in CRISSP so that agencies can review their user lists in between the quarterly audits.[47]

[47] Letter from DHHS to OVIC, 27 June 2019.

Decision to issue a compliance notice

133. As noted above, the Deputy Commissioner found that both the CSP and DHHS breached IPP 4.1.

134. The Deputy Commissioner considered whether the breaches were 'serious' for the purpose of section 78(1)(b)(i) of the PDP Act, and whether a compliance notice should be issued. The Deputy Commissioner considered factors including:

- the type of information in CRISSP;
- the amount of information involved, and the number of people to whom it relates;
- the extent of harm to individuals and the likelihood of further harm that may result from the incident;
- the potential impact of the breach on public trust;
- DHHS's response to the incident and its conduct during the investigation;
- the CSP's response to the incident and its conduct during the investigation;
- the CSP's insight into its culpability regarding the data breach and the steps it has taken in response; and
- DHHS's insight into its culpability regarding the data breach and the steps it has taken in response.

135. In considering these points, the Deputy Commissioner views the breaches as serious, especially given the nature of the information held in CRISSP, the potential consequences for the people the information was about if it were misused, and the ease with which further reasonable steps could have been taken by the CSP and DHHS to negate the potential risk of a breach occurring.

136. With respect to the CSP the Deputy Commissioner considered that a compliance notice was not warranted. Although there were factors both for and against issuing a compliance notice, on balance, the Commissioner decided not to exercise her discretion to issue a compliance notice. A significant contributing factor was the insight and willingness on the part of the CSP to admit to and address the various issues that contributed to the breach. Further, the CSP has acted promptly in response to this investigation and has already implemented new processes and training with respect to off-boarding staff. The Deputy Commissioner considered that ongoing monitoring of the CSP's implementation of the recommendations in the form of a compliance notice was not required.

137. However, with respect to DHHS the Deputy Commissioner considered that a compliance notice was warranted. Although DHHS showed insight and a willingness to admit and address the issues that contributed to the breach, the Deputy Commissioner decided to exercise her discretion to issue a compliance notice. DHHS has received recommendations from other bodies previously with respect to contract management.[48] Further, the recommendations the Deputy Commissioner has made are a large body of work with many complexities due to the nature and size of DHHS, therefore the Deputy Commissioner considered oversight by OVIC

[48] See: Victorian Auditor General's Office, 'Contract Management Capability in DHHS: Service Agreements' (September 2018); Commissioner for Privacy and Data Protection, 'Review of Information Governance Arrangements in the Department of Health and Human Services (DHHS)' (January 2017).

was required. A compliance notice will assist DHHS in ensuring that all recommendations are addressed within a timely manner and will assist in providing confidence from its stakeholders with respect to this issue.

Annexure A

Response from DHHS to investigation

The department has accepted all of the recommendations detailed in OVIC's report and has commenced implementation of those recommendations, including:

- Implementing a risk-tiering framework for managing contracted service providers (including incorporating privacy and information sharing amongst other risks in the tiering process); and
- Commencing implementation of periodic checks of the currency of user lists for CRISSP, including conducting the first check of user lists across all users of CRISSP and to ensure all users of CRISSP are current employees of service providers.

The department takes its privacy and information sharing responsibilities seriously and welcomes OVIC's recommendations to help the department improve its privacy controls.

OVIC's report is a reminder to the department and its many contracted service providers of the importance of having proper systems and controls in place to manage personal information and to mitigate the risk of unauthorised access to such information.

This is especially important in the area of child protection to support the public's trust in this critical function that the department and its service providers provide on a daily basis.

(4 June 2020)

Response from CSP to investigation

The CSP thanks the Office of the Victorian Information Commissioner's (OVIC) for the opportunity to respond to its findings.

The CSP notes, agrees with and has fully implemented the recommendations set out in the report. As a result of this incident it has also taken a range of further internal actions to enhance the protection of personal information in all aspects of its operations.

The CSP exists to make the lives of disadvantaged and at risk clients better and to do this we must build a relationship of trust with a highly vulnerable group. The CSP accepts that the failure to remove XYZ's access to CRISSP may have contributed to harm to those we support.

The CSP accepts that it did not have in place an effective back-up procedure to ensure that the removal of users access to CRISSP was implemented. The CSP has voluntarily implemented a number of internal procedures following the incident to ensure that there are back-up steps in place to ensure that CRISSP access of employees moving roles within the CSP or leaving the CSP is reviewed. The CSP has also implemented a monthly CRISSP access audit to ensure access is up to date and regularly reviewed.

The CSP is committed to protecting the privacy of the individuals whose personal information it holds and has undertaken a comprehensive review led by external consultants of its privacy and data security policies and processes as a result of the incident.

The CSP wishes to record its appreciation for the constructive approach of the Privacy and Data Protection Deputy Commissioner and OVIC's staff to the substantial and significant issues highlighted by this incident and its hope that other CSPs can learn from and apply the recommendations and other findings of this report to reduce the risk of similar incidents in their organisations.

(4 June 2020)

Annexure B

Compliance Notice

COMPLIANCE NOTICE

Under section 78 of the *Privacy and Data Protection Act 2014 (Vic)*

Office of the Victorian Information Commissioner

To: **Department of Health and Human Services**
50 Lonsdale Street
Melbourne Victoria 3000
(the **Organisation**)

I, Rachel Dixon, as empowered by sections 8B(1)(a) and 8C(2)(e) of the *Privacy and Data Protection Act 2014 (Vic)* (the **PDP Act**), serve this compliance notice under Division 9 of Part 3 of the PDP Act.

1. Background

1.1 The Organisation contracted with [NAME REDACTED] (the **CSP**) to deliver its Finding Solutions program.

1.2 To perform these services, authorised employees of the CSP were given access to the Organisation's Client Relationship Information System for Service Providers (**CRISSP**). CRISSP contains personal information about people receiving certain DHHS services.

1.3 Between September 2017 to October 2018 a former employee of the CSP accessed personal information of the CSP's clients while not authorised by either the Organisation or the CSP.

1.4 Under section 8C(2)(e) of the PDP Act, I commenced an investigation into whether the Organisation contravened any Information Privacy Principles in Schedule 1 of the PDP Act.

1.5 Based on this investigation, I was satisfied that the Organisation contravened Information Privacy Principle 4.1 by:

1.5.1 failing to conduct any privacy or security checks on the CSP between 2008 and 2018; and

1.5.2 failing to take steps to confirm the currency of the CRISSP user list between 2008 and 2018.

1.6 I was also satisfied that the contravention was serious.

2. Specified Actions and Periods

2.1 In accordance with section 78(2) of the PDP Act, this compliance notice requires the Organisation to take specified actions within specified periods for the purpose of ensuring compliance with Information Privacy Principle 4.1.

Specified Action 1 – Implementation of a risk-tiering framework

2.2 The Organisation must develop and implement a risk tiering framework for contracted service providers delivering the Finding Solutions program that allows the Organisation to:

2.2.1 assess information security and privacy risks to the organisation from all contracted service providers;

2.2.2 apply tiered risk mitigation strategies and control measures determined by the level of risk that each contracted service provider presents.

2.3 The Organisation must complete Specified Action 1 by 31 March 2021.

2.4 To demonstrate it has completed Specified Action 1, the Organisation must:

2.4.1 report to the Office of the Victorian Information Commissioner (**OVIC**) with evidence of its progress in implementing the risk tiering framework on 30 September 2020; and

2.4.2 provide OVIC evidence that the framework is implemented by 31 March 2021 including by providing supporting governance, policy and operations documents.

Specified Action 2 – Update and simplify its contractual framework and guidance material for CRISSP

2.5 The Organisation must review and update its contractual framework and guidance material for the use of CRISSP by all contracted service providers. The updated material must clearly state the responsibilities of the Organisation and contracted service providers about access to and security of CRISSP.

2.6 The Organisation must complete this Specified Action 2 by 31 March 2021.

2.7 To demonstrate its implementation of Specified Action 2, the Organisation must:

2.7.1 report to OVIC with evidence of its progress in reviewing and updating its contractual framework and guidance material for the use of CRISSP by contracted service providers on 30 September 2020; and

2.7.2 provide to OVIC evidence of an updated contractual framework and guidance material by 31 March 2021.

Specified Action 3 – develop training that is specifically directed at the information security and privacy obligations of systems administrators and Organisation Authorities

2.8 The Organisation must develop and deliver training for all CRISSP users about their information security and privacy obligations when using CRISSP. Training must be delivered to contracted service providers, administrators and Organisation Authorities.

2.9 The Organisation must complete this Specified Action 3 by 31 March 2021.

2.10 To demonstrate its implementation of Specified Action 3, the Organisation must:

2.10.1 report to OVIC with evidence of its progress in developing and delivering training, including a planned schedule of training and copies of training material, on 30 September 2020; and

2.10.2 provide OVIC evidence that training was delivered by 31 March 2021.

Specified Action 4 – implement a procedure to periodically check the currency of user lists for CRISSP

2.11 The Organisation must implement a procedure to regularly check that CRISSP user access is restricted to current, authorised users.

2.12 The Organisation must complete this Specified Action 4 by 30 September 2020.

2.13 To demonstrate its implementation of Specified Action 4, the Organisation must provide details of the procedure and evidence of its implementation to OVIC by 30 September 2020.

3. Enforcement of this compliance notice

3.1 The Organisation must comply with this compliance notice.

3.2 If the Organisation does not comply with this compliance notice, the penalty is:

3.2.1 600 penalty units, in the case of an individual; and

3.2.2 3000 penalty units, in the case of a body corporate.

3.3 If the Organisation considers that it is not reasonably possible to take the action specified in this compliance notice within the period specified, the Organisation may apply to my office before the period of time specified in the compliance notice expires to extend the period of time specified in this compliance notice.

4. Application for review

4.1 An individual or organisation whose interests are affected by my decision to serve this compliance notice may apply to the Victorian Civil and Administrative Tribunal for review of my decision.

Rachel Dixon
Privacy and Data Protection Deputy Commissioner
14 May 2020