Privacy and Personal Information Protection Act 1998

Order

I, Mark Speakman, pursuant to section 31 of the *Privacy and Personal Information Protection Act 1998*, by this order, make the Privacy Code of Practice for the operation of ID Support NSW, the Department of Customer Service, which is annexed to this order, as a privacy code of practice.

M Speakman
Attorney General

Signed at Sydney, this 22nd day of June 2022.

IDSupport NSW Privacy Code of Practice – identity remediation services

1. Overview

1.1. This is a privacy code of practice made under Part 3, Division 1 of the *Privacy and Personal Information Protection Act 1998*. For the purposes of s. 29(5)(c) of the *PPIP Act*, this code applies to the identity remediation activities that IDSupport provides to affected individuals and affected agencies, as set out in this code.

1.2. The *PPIP Act* sets out information protection principles (in Part 2, Division 1) that apply to "public sector agencies" as defined. This code modifies the application of the information protection principles as specified in Section 5 of this code. A public sector agency as described in Section 5 can rely on this code if an information protection principle that applies to it is modified in the circumstances set out in this code.

1.3. A privacy code of practice is not able to affect the operation of any exemption provided under Part 2, Division 3 of the *PPIP Act*. All statutory exemptions remain available to public sector agencies regardless of the provisions of this code.

1.4. This code does not provide authority for any activity that constitutes a criminal offence or is otherwise unlawful. If you are in doubt as to whether any particular handling of information relating to identity security is permitted, please seek legal advice.

1.5. This code will cease to have any application if legislation is enacted that confers information sharing powers on IDSupport that enable it to conduct identity remediation activities.

2. Interpretation

2.1. In this code:

"affected individual" means an individual whose identity information has been compromised as a result of a data compromise

"affected agency" means a public sector agency whose data has been compromised in a data compromise

"compromised data" means identity information that is the subject of a data compromise

"contact details" means information that can be used to contact an individual and includes phone numbers, email addresses, residential addresses and postal addresses

"Core CRM" means the customer relationship management system controlled by IDSupport for use in providing identity remediation services to affected individuals and affected agencies

"CRM" means customer relationship management system

"dark web" means online content that is not indexed by conventional search engines and includes, for example, platforms used for illegal activity such as the trading of identity information

"data compromise" – see [2.2] to [2.5] of this code

"DCS" means the NSW Department of Customer Service

"government issued identity document or credential" means:

- any government issued document (whether in physical or digital form) that contains personal information relating to the person it is issued to, or

- any government issued record (whether in physical or digital form), such as a licence, permit, approval, certificate, registration, authority or other such credential, that provides evidence of the holder's authority, status, rights or entitlement,

which may be used as evidence of identity.

"IDCARE" means the not-for-profit Australian organisation that provides identity compromise support across Australia

"identity information" means information contained in a government issued identity document or credential or other document (whether in physical or digital form) that relates to the identity of a person

"identity remediation services" means the activities set out in Parts 3 and 4 of this code and any ancillary activities

"IDSupport" means IDSupport NSW, the business unit established within DCS as an identity remediation service for affected individuals and public sector agencies

"IPP" means any of the information protection principles set out in Part 2, Division 1 of the *PPIP Act*

"issuing authority" means an organisation that issues government issued identity documents or credentials

"law enforcement agency" has the same meaning as in s. 3 of the *PPIP Act*

"national death data" means the official source of Australian death data accessible through the Queensland Registry of Births, Deaths and Marriages using the Australian Death Check service

"OAIC" means the Office of the Australian Information Commissioner

"affected non-PPIP Act entity" means an entity other than a public sector agency whose data has been compromised in a data compromise, where there is some connection to NSW (for example, an affected individual is a NSW resident or the compromised data includes credentials issued by a NSW issuing authority)

"personal information" has the same meaning as in s. 4 of the *PPIP Act*

"*PPIP Act*" means the *Privacy and Personal Information Protection Act 1998*

"public sector agency" has the same meaning as in s. 3 of the *PPIP Act*

"revoke", in relation to a document or credential, includes cancel or otherwise rescind

"satellite CRM" means the customer relationship management system controlled by an affected agency to enable the agency to manage its response to a data compromise

"up to date contact details" means contact details that are more recent and/or more likely to be accurate than contact details that are already held

2.2. In this code, "data compromise" means:

a) There has been unauthorised access to, or unauthorised disclosure of, personal information held by a public sector agency that may result in harm to an individual to whom the information relates

b) Personal information held by a public sector agency has been lost in circumstances that may result in harm to an individual to whom the information relates

c) There has been use or misuse of personal information by an employee or contracted service provider of a public sector agency in circumstances that may result in harm to an individual to whom the information relates

d) There has been unauthorised access to, or unauthorised disclosure, loss or other misuse of, personal information held by an affected non-PPIP Act entity involving a NSW government issued identity document or credential or the personal information of an individual who resides in NSW

e) There is compromised, unsecured or otherwise exposed identity information available on the internet that includes information about or from a NSW government issued identity document or credential or involves the personal information of an individual who resides in NSW, or

f) There is compromised data stored in an item seized or otherwise obtained by a law enforcement agency or another person or body (whether a public sector agency or not) (for example, where police find identity information stored on laptops or mobile phones that have been seized during the execution of a search warrant) and the compromised data relates to an individual who is a resident of NSW or includes a NSW government issued identity document or credential.

2.3. To avoid doubt, a “data compromise” may occur within a public sector agency, between two or more public sector agencies, within any affected non-PPIP Act entity or by an external person or entity accessing data held by a public sector agency or any affected non-PPIP Act entity without authorisation.

2.4. A data compromise may be apparent from the existence online of compromised data relating to affected individuals.

2.5. A data compromise may be apparent in circumstances where the source of the data compromise is not known.

3. Background

3.1. IDSupport is a business unit established within DCS as an identity remediation service for affected individuals and public sector agencies.

3.2. IDSupport services are available to any person who resides in NSW or who holds a NSW government issued identity document or credential.

3.3. IDSupport reduces the harm caused by misuse of identity information by:

a) Providing a customer identity support function that individuals are referred to, or can contact, for support following the compromise of their identity information, regardless of how or where their identity information has been compromised (which may or may not be known), including by referring individuals to IDCARE or another external contracted service provider to enable individuals to receive specialist support on how to identify risks associated with a data compromise and the action to be taken

b) Providing a whole of government identity support function and a capacity to support and coordinate agency responses to large scale data compromises (including forensic analysis and categorisation of affected individuals, notification of affected individuals and conducting post-incident reviews)

c) Receiving reports about identity information of individuals being available on the dark web and proactively identifying and notifying the individuals to whom this information pertains.

3.4. In the event of a data compromise, IDSupport will:

a) assist affected agencies, when requested to do so, with the review of compromised data to assess the risk of harm to individuals whose identity information is contained within the data

b) use information held by DCS or by another public sector agency where reasonably necessary to assist the affected agency to ascertain or confirm the identity of an individual whose identity information is contained within compromised data

c) advise public sector agencies and affected non-PPIP Act entities about the existence of unsecured or compromised identity information and provide advice on appropriate remediation activities with the affected entity (such as advising affected individuals, assisting with the reissuing of identity documents or credentials or taking steps to improve data security)

d) advise issuing authorities (whether public sector agencies or not) about documents or credentials issued by the authority that have been or may have been compromised, including so that the issuing authority can, where appropriate, suspend, revoke and/or reissue the relevant document or credential, to prevent compromised identity information from being used

e) refer the matter to other bodies where appropriate, such as the NSW Police Force, another public sector agency, an agency of another State or Territory or an agency of the Commonwealth, including where the matter relates to identity crime, and

f) advise the OAIC about data compromises where appropriate.

3.5. IDSupport will also create a “single view of customer” for affected individuals that will be developed within the core CRM and will include information about the individual that IDSupport collects as a consequence of its engagement with the affected individual or in relation to the activities outlined at [3.3] to [3.4]. The single view of customer will enable IDSupport to:

a) assist affected agencies to more rapidly confirm the identity and contact details of affected individuals, for the purpose of providing timely notification to affected individuals.

b) develop a more comprehensive risk profile for individuals affected by multiple data compromises, which can be used to inform a specific assessment of harm undertaken by an agency experiencing a data compromise.

c) enable effective and time-sensitive identity remediation for individuals who are the subject of multiple data compromises or a single compromise that has consequences over a period of time

d) develop policies, guidance, best practice advice and educational services to individuals and public sector agencies about how to minimise the risk and impact of identity compromise on individuals

e) conduct evaluations and other monitoring activities to review the effectiveness of the identity remediation service offered to individuals and public sector agencies.

f) support more comprehensive analysis of the identity compromise risk facing NSW agencies and citizens and a better understanding of the impact of identity compromise and identity-related crime across the NSW community.

3.6. As part of its broader work program, IDSupport will establish three specific pillars of activity that will require the collection, use and disclosure of personal information.

A IDENTITY REMEDIATION SERVICES

3.7. The first pillar will involve IDSupport:

a) assisting an affected agency to undertake its post-compromise response and conduct notification to affected individuals, and

b) providing advice and post-compromise remediation support to individuals affected by the compromise who have received notification in relation to the compromise and have contacted IDSupport for advice and assistance.

3.8. In some circumstances, IDSupport will take steps on behalf of affected individuals in relation to government issued identity documents or credentials that have been impacted by the data compromise.

B DATA COMPROMISES INVOLVING OTHER ENTITIES

3.9. The second pillar will involve providing support to individuals impacted by data compromises involving affected non-PPIP Act entities, including government agencies in other jurisdictions and private sector entities, where the individual is a resident of NSW or the compromised data involves a NSW government issued identity document or credential.

C TAKING ACTION IN RESPONSE TO UNSECURED INFORMATION

3.10. The third pillar will involve IDSupport undertaking specific action as set out below in relation to compromised, unsecured or otherwise exposed identity information that is available as a result of data compromises. This includes information that is available on the internet (including in dark web repositories) and information that has come to the attention of law enforcement agencies, for example when seizing evidence of offences relating to identity crime, who have asked IDSupport for assistance. IDSupport may be notified of the existence of such information by an affected individual, an affected agency, an issuing authority, a law enforcement agency, a law enforcement body of another State or Territory or the Commonwealth, a third party (such as IDCARE), another public sector agency or another part of DCS (including Cyber Security NSW).

4. Process

4.1. IDSupport has been established to provide a single point of service for all NSW residents and holders of NSW government issued identity documents or credentials that have been impacted by a data compromise involving their personal information, regardless of the source of thecompromise.

CRM ARCHITECTURE

4.2. IDSupport has developed CRM architecture to enable IDSupport to provide case management services to affected individuals and affected agencies without accessing more than minimal personal information of affected individuals. The CRM architecture is based in a cloud environment and comprises:

a) The core CRM, access and security of which is controlled by IDSupport, that stores basic personal information of affected individuals, generic descriptors of identity information that has been compromised and basic details of data compromises that have occurred.

b) The satellite CRMs, which are controlled by the affected agencies, that the affected agencies can use to manage their respective responses to a data compromise. A satellite CRM is run within each affected agency's technology stack based on a template developed and provided by IDSupport.

The core CRM

4.3. IDSupport stores the following information on the core CRM:

a) Basic personal information of affected individuals (name, date of birth, contact details such as phone number, email address and residential address, and a unique identifier, if any, allocated by an affected agency) which are updated from time to time as required

b) A generic description of the compromised data for each data compromise that affects the individual (eg "driver licence – yes", "Medicare – no") but not specific identity information (eg individual driver licence number, individual Medicare number), and

c) Details about each data compromise that affects an affected individual (the date of the data compromise, the agency or agencies that were affected, and the details of notification – date, channel and response).

4.4. IDSupport will only create a case record for an affected individual on the core CRM in the following circumstances:

a) An individual who is either a resident of NSW or who holds a NSW government issued identity document or credential contacts IDSupport for assistance

b) An affected agency requests assistance from IDSupport and provides IDSupport with a data set containing personal information of affected individuals, for the purposes of IDSupport providing case management services in response to the data compromise, or

c) IDSupport is provided with or otherwise obtains a data set containing compromised data and the source of the data compromise is not known, or there is no other appropriate entity to respond to the data compromise, and the compromised data relates to residents of NSW or includes NSW government issued identity documents or credentials.

4.5. The core CRM includes a single view of customer function that enables IDSupport to develop a risk profile of individuals who are impacted by multiple data compromises, which in turn enables IDSupport to develop better post-compromise guidance and support for affected individuals who are impacted by multiple data compromises.

4.6. The core CRM is only to be accessible to IDSupport staff and includes specific access controls and auditing functions.

The satellite CRM

4.7. Where an affected agency hosts a satellite CRM, the affected agency holds and controls the information contained within it and retains authority over decisions about what type or types of personal information is stored within it.

4.8. IDSupport does not have access to satellite CRMs. However, the affected agency may disclose personal information held within its satellite CRM to IDSupport for the following purposes, when it is reasonably necessary to do so to enable IDSupport to:

a) Confirm or ascertain the identity of an affected individual

b) Confirm or ascertain up to date contact details of an affected individual

c) Authenticate the identity of an individual who contacts IDSupport in relation to a data compromise

d) Confirm the specific details of how an individual has been impacted by a data compromise, in order to deliver tailored and effective post-compromise support to that individual, or

e) Ascertain whether an affected individual is deceased.

A IDENTITY REMEDIATION SERVICES

When an affected agency requests assistance from IDSupport

4.9. When an affected agency requests assistance from IDSupport with a data compromise, IDSupport compares the basic personal information provided by the affected agency with the data that is already on the core CRM and provides a recommended response to the affected agency (having regard to all of the information that it holds about an affected individual, including any other related data compromises).

4.10. In the case of any discrepancy between the basic personal information that is provided by the affected agency and the data that is already on the core CRM, IDSupport will determine, based on the information available to it, what is likely to be the most accurate and will either update the information on the core CRM accordingly or provide the information that it considers the most accurate, including any up to date contact details of affected individuals that it holds, to the affected agency.

Confirming or ascertaining the identity and/or contact details of affected individuals

4.11. Where an affected agency requests assistance with confirming or ascertaining the identity or contact details of affected individuals, IDSupport may need to cross reference information it holds with information held by another public sector agency or information held by another part of DCS in order to ascertain or confirm the identity and/or contact details of the affected individuals.

4.12. IDSupport will only conduct such cross referencing activities in the following circumstances, and according to the following process:

(a) IDSupport will only conduct a cross referencing activity when there is some doubt as to the identity or contact details of an affected individual, and the cross referencing activity is likely to result in the identity or contact details of the affected individual being ascertained or confirmed.

(b) When IDSupport undertakes a cross referencing activity, it will seek the minimum information necessary to be able to undertake the cross referencing activity that is likely to result in the identity or contact details of the affected individual being ascertained or confirmed.

(c) The information that IDSupport may seek in order to undertake a cross referencing activity is limited to the name, contact details, date of birth, date of death (if applicable) and any other relevant unique identifier (including a reference number for a NSW government issued identity document or credential, such as a NSW driver licence number), that is necessary to confirm or ascertain the identity or contact details of an affected individual, as determined by IDSupport on a case by case basis.

(d) When IDSupport seeks information from another public sector agency or another part of DCS in order to conduct a cross referencing activity, it will share the minimum information necessary to enable the recipient to identify and provide the information sought.

4.13. For certainty, IDSupport may disclose a reference number for a NSW government issued identity document or credential with the relevant issuing authority, for the purpose of ascertaining or confirming the contact details of an affected individual, and the issuing authority may provide IDSupport with the information requested, for the purpose of IDSupport or the affected agency notifying the affected individual of the data compromise.

Ascertaining whether an affected individual is deceased

4.14. If an affected agency requests assistance from IDSupport with ascertaining whether affected individuals are deceased, IDSupport will ask the affected agency to consider whether the details of all individuals affected by the data compromise, or just a subset of certain cohorts, should be disclosed to IDSupport for this purpose. IDSupport will ask the affected agency to consider the following criteria:

a) The date of the records containing the personal information

b) The date or dates of the affected individual’s interactions with the affected agency, including the date of the most recent information on the affected individual held by the affected agency, and

c) Any other relevant factors, as determined by IDSupport and/or the affected agency.

4.15. Following that assessment, the affected agency may disclose to IDSupport the full name and date of birth of such affected individuals as the affected agency considers should be included in the request, for the purpose of IDSupport ascertaining whether any of those affected individuals are deceased.

4.16. IDSupport will then share this information with the NSW Registry of Births Deaths and Marriages, who will check any relevant records it has access to, including national death data, and notify IDSupport if any of the affected individuals included in the request are deceased. Alternatively, IDSupport will check national death data itself to determine whether any of the affected individuals included in the request are deceased. IDSupport will then disclose the details of any deceased individuals to the affected agency. The affected agency will retain the discretion as to whether to proceed with notification of the family or other next of kin, should relevant contact details be available to the affected agency.

4.17. Where the affected agency is DCS, the part of DCS that is affected by the data compromise may request assistance from IDSupport with ascertaining whether affected individuals are deceased, as set out above at [4.14] to [4.16], as if the references to the affected agency are references to the part of DCS that is affected by the data compromise.

Responsibility for responding to data compromises

4.18. Affected agencies (not IDSupport) are responsible for determining whether or not they are legally obliged to notify affected individuals about a data breach and whether or not they are going to notify affected individuals about data compromises. Affected agencies are responsible for notifying affected individuals about data compromises, including on behalf of other affected agencies, where there has been a data compromise involving multiple agencies and a coordinated response is appropriate and agreed.

When an affected individual requests assistance from IDSupport

4.19. When an affected individual requests assistance from IDSupport, IDSupport will handle the individual’s personal information in accordance with the information protection principles.

4.20. As part of IDSupport’s interaction with an individual who has requested assistance from IDSupport, IDSupport will collect personal information from the individual for the purposes of:

a) Verifying the identity of the individual

b) Ascertaining or confirming whether the individual has been affected by a NSW government data compromise, and

c) Developing a post-data compromise risk profile for the individual, which will inform any post-compromise advice or assistance that IDSupport subsequently provides to the individual.

4.21. If an affected individual requests assistance from IDSupport, IDSupport may use identity verification processes to ensure that the individual is who they say they are, before providing any identity remediation services to the individual. IDSupport may collect or otherwise obtain photographs and/or other identity documents from the individual, in order to verify the individual's identity. Any such identity verification process will only be conducted with the express consent of the individual seeking the identity remediation services.

B DATA COMPROMISES INVOLVING AFFECTED NON-PPIP ACT ENTITIES

4.22. Where an individual is affected by a data compromise involving an affected non-PPIP Act entity IDSupport will initiate an individual record on the core CRM only when the individual contacts IDSupport for assistance or advice in relation to the data compromise.

4.23. IDSupport will collect personal information from the affected individual directly or, with the individual's consent, from a third party (unless the collection is otherwise permitted under privacy law).

4.24. Personal information obtained by IDSupport may be used to develop a single view of customer only with the consent of the affected individual (unless the use is otherwise permitted under privacy law).

4.25. IDSupport may use or disclose personal information collected from an individual where this is reasonably necessary for the purpose of assisting the individual to take steps to prevent their identity information being further compromised or otherwise misused. Personal information will be used or disclosed only with the consent of the affected individual (unless the use or disclosure is otherwise permitted under privacy law).

C TAKING ACTION IN RESPONSE TO UNSECURED INFORMATION

4.26. IDSupport may be made aware of compromised, unsecured or otherwise exposed identity information that is available, for example, on the internet (including in dark web data repositories) or in evidence that has been obtained by a law enforcement agency or a law enforcement body of another State or Territory or the Commonwealth. The source of the data compromise may not be known and IDSupport may not be able to identify any affected agency or affected non-PPIP Act entity. When IDSupport is made aware of such information being available, IDSupport will undertake a harm assessment in relation to the information, giving consideration to factors including the following:

a) Whether the exposed identity information has likely been disclosed intentionally by the individual to whom it relates or lawfully by a third party

b) Whether the exposed identity information could be used to cause harm to the individual to whom it relates, including by being used for malicious purposes such as identity theft or fraud, and

c) Whether the exposed identity information is visible or could be accessed by third parties.

4.27. If, upon assessment, IDSupport determines that there is a risk of harm to the individuals to whom the exposed identity information relates, IDSupport may take such steps, as are reasonably necessary in the circumstances, to obtain a copy of it or of part of it. Before doing so, IDSupport may seek legal advice or may seek assistance or advice from the NSW Police Force, Cyber Security NSW or another appropriate organisation. IDSupport will not collect any information by unlawful means.

4.28. Where IDSupport obtains the data set containing the exposed personal information, or part of it, IDSupport may compare the exposed personal information with other personal information held on the core CRM for the purpose of confirming the identity and contact details of the affected individuals.

4.29. IDSupport may need to cross reference information it holds with information held by other public sector agencies or information held by another part of DCS in order to ascertain or confirm the identity or contact details of affected individuals. IDSupport will only conduct such cross referencing activities in accordance with the process set out above at [4.11] to [4.13].

4.30. IDSupport may ascertain whether an affected individual is deceased in accordance with the process set out above at [4.14] to [4.16].

TAKING ACTION TO PROTECT DOCUMENTS AND CREDENTIALS

NSW government issued identity documents and credentials

4.31. Should IDSupport conclude, based on information available to it, that there is a risk that a NSW government issued identity document or credential has been, or may be, subject to misuse, it may convey this assessment (including its reasons for making the assessment and any information on which the assessment was based) to the issuing authority on behalf of the affected individual and request that the document or credential should:

a) have an alert be placed on its use or be suspended, and/or

b) be revoked and/or reissued.

4.32. IDSupport will generally only make such a request with the consent of the affected individual, either because:

a) The affected individual is in contact with IDSupport and has requested IDSupport's assistance

b) The affected individual is in contact with the affected agency (where applicable) and the affected agency has requested IDSupport's assistance on behalf of the affected individual, or

c) IDSupport has formed the view independently of any interaction with the affected individual that action in relation to a NSW government issued identity document or credential is warranted, and has contacted the affected individual for the purpose of obtaining the affected individual's consent, and has obtained that consent.

4.33. However, if IDSupport or the affected agency (where relevant) is unable to contact the affected individual, or the affected individual does not respond to a request for consent, or IDSupport is not able to verify the identity of the affected individual, IDSupport may:

a) obtain the full details of the relevant NSW government issued identity document or credential from the affected agency (where applicable)

b) disclose these details to the issuing authority that issued the identity document or credential

c) provide the issuing authority with a specific request to have an alert or suspension placed on its use, and/or to have it revoked and/or reissued, outlining relevant information supporting this request in accordance with any requirements of the issuing authority

d) document the justification for the action taken by IDSupport on the core CRM

e) document the outcome of the request within the relevant record on the core CRM, and

f) take all reasonable steps to communicate the outcome of this request to the affected individual and the affected agency.

4.34. IDSupport will not take steps to protect a NSW government issued identity document or credential on behalf of an affected individual in the absence of the affected individual's consent unless, in the view of IDSupport, such steps are warranted because there is a real risk of the document or credential being misused by a third party. IDSupport may take into account any relevant information available to it when considering whether or not such steps are warranted, including:

a) The circumstances of the data compromise, including whether the data compromise was the result of criminal activity, including cyber activity

b) The likelihood of the identity documents or credentials being in the possession of, or accessible to, third parties

c) Whether the identity document or credential could be used for criminal purposes, such as identity theft, identity-enabled or impersonation fraud or other misuse that would cause harm to the affected individual, and

d) Whether there is any evidence that the identity document or credential has been, or is likely to be, used for criminal purposes such as identity theft, identity-enabled or impersonation fraud.

4.35. Whether to take action in response to a request by IDSupport is a matter for the issuing authority, in light of its powers and functions.

Government issued identity documents and credential – other jurisdictions

4.36. In circumstances where an identity document or credential issued by a government of another State or Territory or the Commonwealth has been compromised, IDSupport may take action as follows:

a) If the government issued identity document or credential was compromised as a result of a data compromise involving a public sector agency, and an affected individual receives notification of this data compromise and contacts IDSupport for assistance in relation to the affected documents or credentials, IDSupport may provide support in accordance with the process outlined at [4.31] to [4.35].

b) If the government issued identity document or credential was compromised other than as a result of a data compromise involving a public sector agency, IDSupport may provide support in accordance with the process outlined at [4.31] to [4.35] or may limit its assistance to advice only.

RETENTION AND STORAGE OF INFORMATION

4.37. IDSupport will store personal information of affected individuals either:

a) On the core CRM, as set out at [4.3 – 4.6], or

b) On the DCS corporate network, in segregated directories only accessible to IDSupport staff and which are subject to security, access and auditing controls that are appropriate for the information stored within the directories.

4.38. IDSupport has undertaken a security risk assessment of its CRM environment and will undertake related security assurance processes on a periodic basis. IDSupport will implement further security and access controls (including, where appropriate, encryption and further network segregation) to provide additional protection to specific data, including any bulk data sets containing digital copies of identity documents or credentials. IDSupport will implement any further security and access controls that are deemed appropriate by the IDSupport Director or DCS Chief Information Security Officer.

4.39. Any personal information that is stored on the core CRM will be retained in accordance with state records obligations and then deleted or otherwise disposed of securely. Information on the core CRM that is not personal information (including personal information that has been de-identified) may be retained indefinitely.

4.40. Any personal information that is stored other than on the core CRM will also be retained in accordance with state records obligations and then deleted or otherwise disposed of securely.

ALERTING ENTITIES TO THE FACT THERE HAS BEEN A DATA COMPROMISE

NSW public sector agencies

4.41. Where IDSupport receives notification of a data compromise other than from an affected agency, DCS can notify the affected agency of the data compromise and can share information about the data compromise with the affected agency.

4.42. IDSupport will only share personal information with the affected agency where provision of the information is reasonably necessary in the circumstances to assist the affected agency to contain or investigate the incident (including by ascertaining its location and scope) or to identify and notify affected individuals.

4.43. This may include information from the core CRM and/or personal information contained within the compromised data set, or a sub-set of it, to the extent that the provision of this information is reasonably necessary to assist the affected agency to contain or investigate the incident (including by ascertaining its location and scope) or to identify and notify affected individuals.

Government agencies in other jurisdictions and private entities

4.44. Where IDSupport receives notification of, or otherwise becomes aware of, a data compromise that affects an affected non-PPIP Act entity, DCS can alert the entity to the data compromise and/or refer the matter to IDCARE.

4.45. IDSupport will generally disclose to the affected non-PPIP Act entity personal information about individuals affected by the data compromise only when it has the consent of the individual to do so.

4.46. However, in circumstances where further specific information is requested by the affected non-PPIP Act entity to contain or investigate the data compromise, or to identify and notify affected individuals, IDSupport may disclose limited personal information about affected individuals to the affected non-PPIP Act entity. This information should be restricted to initial and surname for a subset of individuals contained within the compromised data set.

SHARING INFORMATION OUTSIDE NSW OR WITH COMMONWEALTH AGENCIES (*PPIP Act*, s. 19(2))

4.47. IDSupport may wish to share information with a person or body who is in a jurisdiction outside NSW, or to a Commonwealth agency. For example:

a. Where IDSupport receives notification of, or otherwise becomes aware of, a data compromise that affects an entity that is a person or body in another State or Territory or is a Commonwealth agency, IDSupport can alert the entity to the data compromise.

b. IDSupport may notify an issuing authority that is a Commonwealth agency or an agency of another State or Territory that documents or credentials it has issued have been compromised and may share information with the issuing authority for that purpose.

c. IDSupport may ask an issuing authority that is a Commonwealth agency or an agency of another State or Territory to suspend, revoke and/or reissue a document or credential that has been compromised and may share information with the issuing authority for that purpose.

d. IDSupport may share information with a law enforcement body of another State or Territory or the Commonwealth in connection with IDSupport providing identity remediation services to or otherwise supporting the affected individuals or the affected agency, in circumstances where identity theft or other identity-related fraud has been or appears to have been committed.

4.48. Before IDSupport discloses personal information to a person or body who is in a jurisdiction outside NSW, or to a Commonwealth agency, IDSupport will take reasonable steps to ensure that the information will not be held, used or disclosed by the recipient of the information inconsistently with the information protection principles, unless there is another legal basis on which the information can be disclosed to the recipient.

5. Modification of information protection principles

5.1. The application of the information protection principles set out in Part 2, Division 1 of the *PPIP Act* to public sector agencies is modified as follows.

5.2. **IPP 2** (section 9) is modified as follows:

(a) DCS need not collect information directly from the individual to whom it relates when IDSupport:

(i) Receives notifications of data compromises from affected agencies, affected non-PPIP Act entities, issuing authorities, police, IDCARE, other third parties or other parts of DCS

(ii) Seeks information from another public sector agency where necessary to enable IDSupport to undertake cross referencing activities in order to identify with confidence the identity of individuals affected by a data compromise, in accordance with the process set out in Part 4 of this code

(iii) Receives up to date contact details of affected individuals from another public sector agency, in accordance with the process set out in Part 4 of this code

(iv) Receives a request from an affected agency to help ascertain whether any affected individuals are deceased

(v) Receives information as to whether an affected individual is deceased, in accordance with the process set out in Part 4 of this code

(vi) Receives information for inclusion on the core CRM (namely, basic personal information of affected individuals, a generic description of the compromised data for each compromise that affects an affected individual and details about each compromise that affects that individual)

(vii) Receives a response to a request it makes to an issuing authority to suspend, revoke and/or reissue a document or credential

(viii) Receives information from the NSW Police Force or another law enforcement agency (or a law enforcement body of another State or Territory or the Commonwealth) for the purpose of IDSupport providing identity remediation services to or otherwise supporting the affected individuals or the affected agency, in circumstances where identity theft or other identity-related fraud has been or appears to have been committed, or

(ix) Obtains a copy or part of a copy of compromised, unsecured or otherwise exposed identity information, in accordance with the process set out in Part 4 of this code.

(b) A public sector agency other than DCS need not collect information directly from the individual to whom it relates when it:

(i) Receives a request from IDSupport for up to date contact details of affected individuals

(ii) Receives up to date contact details of affected individuals or any recommended response to a data compromise from IDSupport

(iii) Receives notification of a data compromise from IDSupport

(iv) Receives information from IDSupport, where IDSupport is undertaking cross referencing activities in order to identity with confidence the identity of the individuals affected by a data compromise

(v) Receives information from the core CRM from IDSupport to assist in its response to a data compromise, or

(vi) Receives a request from IDSupport to suspend, revoke and/or reissue a document or credential.

(c) A public sector agency that is an issuing authority need not collect information directly from the individual to whom it relates when it receives a request from IDSupport or an affected agency to suspend, revoke and/or reissue a document or credential.

5.3. **IPP 10** (section 17) is modified as follows:

(a) There is no intention to depart from s. 17 where an affected agency provides information to DCS for the purpose of IDSupport providing identity remediation services, and DCS uses it for that purpose.

(b) For certainty, IDSupport can undertake cross referencing activities using information that it holds and information that has been obtained from another public sector agency for that purpose so that it can determine with confidence the identity of individuals affected by a data compromise, in accordance with the process set out in Part 4 of this code.

(c) For certainty, IDSupport can make inquiries with the NSW Registry of Births Deaths and Marriages, or make inquiries itself, for the purpose of ascertaining whether an affected individual is deceased, in accordance with the process set out in Part 4 of this code.

(d) Where DCS is the affected agency, the part of DCS that is affected by the data compromise can notify IDSupport about the data compromise. It can share information for inclusion on the core CRM (namely, basic personal information of affected individuals, a generic description of the compromised data for each compromise that affects an individual and details about each compromise that affects that individual).

(e) A part of DCS that holds an affected individual’s up to date contact details can provide those details to IDSupport upon request, for the purpose of IDSupport providing identity remediation services to an affected agency or the affected individual.

(f) Where a government issued identity document or credential has been compromised, and DCS is the issuing authority, IDSupport may request the part of DCS that issued the document or credential to suspend, revoke and/or reissue it, and the part of DCS that issued the document or credential may receive that request and provide a response to IDSupport.

(g) DCS can use personal information it collects through IDSupport’s provision of identity remediation services to form a single view of customer and can have regard to the single view of customer and other information on the core CRM when formulating recommended responses to provide to affected agencies or (where DCS is the affected agency) to the part of DCS that is affected by the data compromise.

(h) An affected agency can use personal information that it holds to notify affected individuals of a data compromise.

5.4. **IPP 11** (section 18) is modified as follows:

(a) Where IDSupport receives notification of a data compromise other than from an affected agency, DCS can notify the affected agency of the data compromise in accordance with the process set out in Part 4 of this code.

(b) Where IDSupport receives notification of, or otherwise becomes aware of, a data compromise that affects an affected non-PPIP Act entity, DCS can alert the entity to the data compromise and/or refer the matter to IDCARE. Where IDSupport alerts the affected non-PPIP Act entity of the data compromise, it may do so in accordance with the process set out in Part 4 of this code.

(c) Where IDSupport receives notification of a data compromise, and needs to undertake cross referencing activities using information it holds and information that is held by another public sector agency in order to identify with confidence the identity of individuals affected by a data compromise:

(i) DCS can disclose information to the other public sector agency for that purpose, in accordance with the process set out in Part 4 of this code, and

(ii) The other public sector agency can disclose information to DCS for that purpose.

(d) Where IDSupport seeks information from another public sector agency, and the provision of the information is necessary to enable IDSupport to undertake cross referencing activities in order to identify with confidence the identity of individuals affected by a data compromise, the public sector agency may disclose the information to IDSupport.

(e) DCS can disclose information to an affected agency to confirm whether an affected individual is deceased.

(f) DCS can disclose information from the core CRM to an affected agency when IDSupport provides the affected agency with a recommended response to the agency's data compromise.

(g) DCS can disclose an affected individual's up to date contact details to an affected agency to enable the agency to notify the individual of the agency's data compromise.

(h) A public sector agency can disclose an affected individual's up to date contact details to DCS upon request by IDSupport to enable DCS to provide the individual's up to date contact details to an affected agency.

(i) DCS may notify an issuing authority (whether it is a public sector agency or not) that documents or credentials it has issued have been compromised and may share information with the issuing authority for that purpose.

(j) DCS may ask an issuing authority to suspend, revoke and/or reissue a document or credential that has been compromised, in accordance with the process set out in Part 4 of this code, and may share information with the issuing authority for that purpose.

(k) A public sector agency that is an affected agency may share information with an issuing authority in order to request that the issuing authority suspend, revoke and/or reissue a document or credential that has been compromised.

(l) DCS may share information with the NSW Police Force or another law enforcement agency or a law enforcement body of another State or Territory or the Commonwealth in connection with IDSupport providing identity remediation services to or otherwise supporting the affected individuals or the affected agency, in circumstances where identity theft or other identity-related fraud has been or appears to have been committed.

(m) DCS may notify the OAIC of a data compromise involving an APP entity as defined by the *Privacy Act 1988*, or refer a matter to the OAIC, as appropriate.

(n) An affected agency may provide IDSupport with information for inclusion on the core CRM as specified in paragraph [4.3] of this code.

6. Review

6.1. DCS will review this code 12 months after it comes into effect and will report to the Privacy Commissioner on the outcome of that review. The report to the Privacy Commissioner will include information about action taken under the code and assurance activities that DCS has taken to ensure compliance with the code.