Government of South Australia

Privacy Committee of South Australia

2017-18 Annual Report

Privacy Committee of South Australia

GPO Box 464
ADELAIDE SA 5001

Level 17, 45 Pirie Street
ADELAIDE SA 5000

https://archives.sa.gov.au/alias/privacy

Contact phone number (08) 8204 8786

Contact email staterecords@sa.gov.au

ISSN 2208-6110

Date presented to Minister: 28 September 2018

To the Hon Vickie Chapman MP

Deputy Premier

Attorney-General

This annual report is presented to Parliament to meet the reporting requirements of clause 4A of the *Proclamation establishing the Privacy Committee of South Australia* and meets the requirements of Premier and Cabinet Circular *PC013 Annual Reporting*.

This report is verified to be accurate for the purposes of annual reporting to the Parliament of South Australia.

Submitted on behalf of the Privacy Committee of South Australia by:

Simon Froude

Presiding Member, Privacy Committee of South Australia

Signature _____ Date 20/9/18

Contents

Section A: Reporting required under the *Public Sector Act* 2009, the *Public Sector Regulations 2010* and the *Public Finance and Audit Act* 1987

Committee purpose and objectives

The Privacy Committee of South Australia (Privacy Committee) was established by the *Proclamation establishing the Privacy Committee of South Australia* (the Proclamation) in the Government Gazette on 6 July 1989. The functions of the Privacy Committee, as described in the Proclamation, are:

- to advise the Minister as to the need for, or desirability of, legislation or administrative action to protect individual privacy and for that purpose to keep itself informed as to developments in relation to the protection of individual privacy in other jurisdictions.
- to make recommendations to the Government or to any person or body as to the measures that should be taken by the Government or that person or body to improve its protection of individual privacy.
- to make publicly available, information as to methods of protecting individual privacy and measures that can be taken to improve existing protection.
- to keep itself informed as to the extent to which the Administrative Scheme of Information Privacy Principles is being implemented.
- to refer written complaints concerning violations of individual privacy received by it (other than complaints from employees of the Crown, or agencies or instrumentalities of the Crown, in relation to their employment) to the appropriate authority.
- such other functions as are determined by the Minister.

The Privacy Committee may, under clause 4 of the Proclamation, 'exempt a person or body from one or more of the Information Privacy Principles on such conditions as the Privacy Committee thinks fit'.

Legislation (Cabinet Instruction) administered by the Committee

South Australia's *Information Privacy Principles Instruction* (IPPI) was introduced in July 1989 by means of *Cabinet Administrative Instruction 1/89*, issued as *Premier & Cabinet Circular No. 12*. The IPPI includes a set of ten Information Privacy Principles (IPPs) that regulate the way South Australian public sector agencies collect, use, store and disclose personal information.

Organisation of the Committee

Clause 1(2) of the Proclamation of the Privacy Committee establishes the membership of the Committee. It requires that the Committee consists of six members, all of whom are to be appointed by the Minister. Of the six members:

- three are nominated by the Minister (one of whom must not be a public sector employee and one must have expertise in information and records management);
- one is to be nominated by the Attorney-General;
- one is to be nominated by the Minister responsible for the administration of the Health Care Act 2008; and
- one is to be nominated by the Commissioner for Public Employment.

At the conclusion of the reporting year, the membership of the Committee was as follows:

Presiding Member:

- Mr Simon Froude, Director, State Records of South Australia, Attorney-General's Department – appointed to 11 January 2019.

Members, in alphabetical order:

- Ms Kathy Ahwan, Manager, Policy and Legislation, Legal and Legislative Policy Unit, Department of Health and Wellbeing – appointed to 11 January 2019.
- Ms Deslie Billich, non-public sector employee – appointed to 30 September 2020.
- Ms Lucinda Byers, Special Counsel, Office of the Chief Executive, Attorney-General's Department – appointed to 30 March 2019.
- Mr Nathan Morelli, Director | Adelaide Joint Cyber Security Centres (JCSC) Engagement & Awareness Branch – appointed to 29 January 2019.
- Ms Krystyna Slowinski, Principal Internal Auditor, Department for Communities and Social Inclusion – appointed to 1 June 2020.

Change of membership

Ms Slowinski's membership to the Privacy Committee was due to expire during the reporting year. Ms Slowinski agreed to a further term.

Ms Billich whose membership was due to expire in September 2018, also agreed to undertake an additional term.

The Minister approved these reappointments on 29 June 2018.

Committee Remuneration

Premier & Cabinet Circular No. 16: Remuneration for Government Appointed Part-time Boards and Committees specifies the conditions under which members of boards and committees may be remunerated. Only non-government members of the Privacy Committee are entitled to receive a sessional fee for meetings attended. The sessional fees are drawn from State Records' recurrent operating budget. More information about the payment of fees can be found at *Premier & Cabinet Circular No. 16* available on the Premier and Cabinet website.

The sessional rate for applicable members of the Privacy Committee during 2017-18 was $206.

Other agencies related to this agency (within the Minister's area/s of responsibility)

State Records of South Australia provides executive support to the Privacy Committee including research and policy support, administrative support, meeting coordination, web hosting and an enquiry and advice service to agencies and the public.

Section B: Reporting required under any other act or regulation

Exemptions Granted

Clause 4 of the Proclamation establishing the Privacy Committee of South Australia provides that the Privacy Committee may exempt any person or body from one or more of the IPPs on such conditions as the Privacy Committee sees fit.

Clause 4A(2) of the Proclamation provides that the Privacy Committee's Annual Report '*must include details of any exemption granted under clause 4 during the year to which the report relates*'.

Exemption – Offender Management Program – Aboriginal Advisors

This exemption applies to the South Australia Police (SAPOL), Department for Correctional Services (DCS), Department for Communities and Social Inclusion (DCSI), SA Health, Attorney-General's Department (AGD), Department of State Development (DSD), and TAFE SA. It is an exemption from compliance with IPPs 2, 8 and 10, allowing SAPOL, DCS, DCSI, AGD, DSD and TAFE SA to share case file information of serious offenders as part of the Offender Management Plan Program (OMP Program). It is an exemption from compliance with IPPs 2 and 8 allowing SA Health to share case file information of serious offenders as part of the OMP Program.

The personal information to be shared is case file information and other personal information relevant to offenders included in the OMP Program. This includes the personal information of family members and associates, where it has been identified that those individuals contribute significantly to the offending lifestyle of the nominated offender. The information is collected and held by each agency through its mandated service provision.

The purpose of the collection, use and disclosure of the personal information is to allow the successful functioning of the OMP Program in providing coordinated case management of selected serious offenders to reduce recidivism and promote community safety. This exemption also provides for the disclosure of relevant personal information to third party service providers necessary for the provision of targeted services to individual offenders under the OMP Program.

This exemption specifically provides for the sharing of personal information to Aboriginal Advisors, employed by DCSI's Exceptional Needs Unit, who will support the OMP Ceduna Program in an advisory capacity.

All other Principles continue to apply.

<u>Conditions</u>

This exemption is conditional on the following:

- personal information shared through the OMP Program is only used for the purposes of coordinated case management of selected serious offenders; and
- individual offenders are informed of their inclusion in the OMP Program; and
- the Guidelines for the OMP Program are amended to include clear pathways for complaints relating to the use of personal information; both internally and externally; and

- a system for monitoring and recording breaches of personal information privacy is implemented; and
- consent is sought from family members and associates, where it has been identified that those individuals contribute significantly to the offending lifestyle of the nominated offender, for their personal information to be shared as part of the OMP Program. Only in circumstances where consent is not granted, or if it is given and then later revoked, does this exemption apply.

Security of Personal Information

The security of the personal information should be managed in line with the Government's Protective Security Management Framework (Premier and Cabinet Circular 30) and Information Security Management Framework, and the agency's security management systems and practices. Participating agencies must specifically ensure that:

- steps taken to secure personal information are proportionate to its sensitivity and the risk of its loss or misuse;
- personal information is kept in a secure area within participating agencies;
- personal information is protected during transit;
- electronic information should be encrypted and password protected and physical files should not be left unattended in an unsecure environment; and
- access to personal information is on a strictly need-to-know basis. Personal information collected under the OMP Program should not be on-disclosed or distributed further within participating agencies for any purposes other than facilitating any actions under a participating offender's case management plan, delivering services to the offender as an existing client or where otherwise allowable under IPPs 8 and 10.

Destruction or retention of personal information

Destruction or retention of the personal information must be undertaken in accordance with a disposal authority under the *State Records Act 1997*.

Expiry

This exemption applies from 27 September 2017 to 30 June 2018.

Exemption – DECD (Preschool enrolment census data)

This revised exemption applies to the Department for Education and Child Development (DECD). It is an exemption from compliance with Principle 10 allowing DECD to disclose identifying information from its preschool enrolment census data for non-government and private schools to SA NT DataLink for the purposes of data linkage.

The personal information to be disclosed will initially be for the period between 2012 and 2017, representing approximately 110,000 students. Annual updates will then be sought, with an expectation that each update will include approximately 18,500 new students.

The personal information and linkage variables includes:

Record identifier, Personal identifier, Names – all names including nicknames, aliases and aka, Date of birth, Sex, Aboriginality, Torres Strait Islander Indicator Country of birth, Full address including geocodes if available, Site name, Site ID and Census year

The purpose of disclosing this information is to enable a more complete understanding of the early childhood sector and pathways in child health and development when developing policy, research and strategic plans.

All other Principles continue to apply.

Conditions

The information is only to be used for the creation of master linkage keys in the further development of the master linkage file as part of the Data Linkage System. The exemption is provided on the condition that the personal information is only to be accessed by officers of SA Health within the Data Linkage Unit.

DECD remains responsible for the secure transfer of personal information in line with the IPPs.

This exemption is conditional on SA NT DataLink having a current Joint Venture Consortium Agreement in place.

Destruction or retention of personal information

Destruction or retention of the personal information must be undertaken in accordance with a disposal authority under the *State Records Act 1997*.

Expiry

This exemption is granted from 28 February 2018 to 31 March 2021. An extension may be negotiated with the Privacy Committee if required.

Exemption – DPTI (Sanitary drain drawings)

This exemption applies to the Department of Planning, Transport and Infrastructure / LocationSA and concerns the personal information contained in drawn representations of the underground on-site sanitary plumbing work within a specific property (the sanitary drain drawings).

Specifically the personal information consists of the name of persons who currently or previously owned a property, the address of that property, the name and contact details of the plumber who undertook plumbing work to install the sanitary drains on the property and the location of sanitary drains on the property.

The agency is granted an exemption from Principle 10 for the purpose of disclosing the sanitary drain drawings to the public.

All other Principles continue to apply.

Conditions

This exemption is granted on the condition that:

- where possible the name of the property owner and name and contact details of the plumber are deleted from the drawings prior to release to the public
- the agency in collaboration with the Department of Premier and Cabinet, Office of the Technical Regulator take all necessary steps to put in place a process whereby a person can apply to have the sanitary drain drawing of a property that he or she owns, or lives in, suppressed from access by the public.

Security

The security of the personal information should be managed in line with the Government's Protective Security Management Framework (Premier and Cabinet Circular 30) and Information Security Management Framework, and the agency's security management systems and practices.

Destruction or retention of personal information

Destruction or retention of the personal information must be undertaken in accordance with a disposal authority under the *State Records Act 1997*.

Expiry

This exemption is granted from 1 March 2018 to 31 May 2018. A further extension may be negotiated with the Committee if required.

Exemption – DPC (Sanitary drain drawings)

This exemption applies to the Department of the Premier and Cabinet (DPC) and concerns the personal information contained in drawn representations of the underground on-site sanitary plumbing work within a specific property (the sanitary drain drawings) held by the Office of the Technical Regulator.

Specifically the personal information consists of the name of persons who currently or previously owned a property, the address of that property, the name and contact details of the plumber who undertook the plumbing work to install the sanitary drains on the property and the location of sanitary drains on the property.

The agency is granted an exemption from compliance with Principles 6 and 9 in relation to the drawings.

The agency is also granted an exemption from Principle 10 for the purpose of disclosing the drawings:

- to the public
- to the Department of Planning, Transport and Infrastructure (DPTI) for the purpose of creating on-line access to the drawings by the public.

All other Principles continue to apply.

Conditions

This exemption is granted on the condition that:

- the process of collecting the sanitary drain drawings is amended such that the name of the property owner and the name and contact details of the plumber is no longer required to be supplied
- where possible the name of the property owner and name and contact details of the plumber are deleted from the sanitary drain drawings prior to release to DPTI or the public
- the agency take the lead on establishing a process whereby a person can apply to have the sanitary drain drawing of a property that he or she owns, or lives in, suppressed from access by the public.

DPC is responsible for the secure transfer of personal information in line with the IPPs.

Security

The security of the personal information should be managed in line with the Government's Protective Security Management Framework (Premier and Cabinet Circular 30) and Information Security Management Framework, and the agency's security management systems and practices.

Destruction or retention of personal information

Destruction or retention of the personal information must be undertaken in accordance with a disposal authority under the *State Records Act 1997*.

Expiry

This exemption is granted from 1 March 2018 to 31 May 2018. A further extension may be negotiated with the Committee if required.

Exemption – DPC/DEM (Sanitary drain drawings)

This exemption applies to the Department of the Premier and Cabinet (DPC)/Department for Energy and Mining (DEM) and concerns the personal information contained in drawn representations of the underground on-site sanitary plumbing work within a specific property (the sanitary drain drawings) held by the Office of the Technical Regulator.

Specifically the personal information consists of the name of persons who currently or previously owned a property, the address of that property, the name and contact details of the plumber who undertook the plumbing work to install the sanitary drains on the property and the location of sanitary drains on the property.

The agency is granted an exemption from compliance with Principles 6 and 9 in relation to the drawings.

The agency is also granted an exemption from Principle 10 for the purpose of disclosing the drawings:

- to the public
- to the Department of Planning, Transport and Infrastructure (DPTI) for the purpose of creating on-line access to the drawings by the public.

All other Principles continue to apply.

Conditions

This exemption is granted on the condition that:

- where possible the name of the property owner and name and contact details of the plumber are deleted from the sanitary drain drawings prior to release to DPTI or the public
- the process is maintained that allows a person to apply to have the sanitary drain drawing of a property that he or she owns, or lives in, suppressed from access by the public.

DPC/DEM is responsible for the secure transfer of personal information in line with the IPPs.

Security

The security of the personal information should be managed in line with the Government's Protective Security Management Framework (Premier and Cabinet Circular 30) and Information Security Management Framework, and the agency's security management systems and practices.

Destruction or retention of personal information

Destruction or retention of the personal information must be undertaken in accordance with a disposal authority under the *State Records Act 1997*.

Expiry

This exemption is granted from 1 June 2018 to 31 May 2021. A further extension may be negotiated with the Committee if required.

Exemption – DPTI (Sanitary drain drawings)

This exemption applies to the Department of Planning, Transport and Infrastructure / LocationSA and concerns the personal information contained in drawn representations of the underground on-site sanitary plumbing work within a specific property (the sanitary drain drawings).

Specifically the personal information consists of the name of persons who currently or previously owned a property, the address of that property, the name and contact details of the plumber who undertook plumbing work to install the sanitary drains on the property and the location of sanitary drains on the property.

The agency is granted an exemption from Principle 10 for the purpose of disclosing the sanitary drain drawings to the public.

All other Principles continue to apply.

Conditions

This exemption is granted on the condition that:

- where possible the name of the property owner and name and contact details of the plumber are deleted from the drawings prior to release to the public
- the agency in collaboration with the Office of the Technical Regulator, Department of the Premier and Cabinet/Department of Energy and Mining, take all necessary steps to maintain the process whereby a person can apply to have the sanitary drain drawing of a property that he or she owns, or lives in, suppressed from access by the public.

Security

The security of the personal information should be managed in line with the Government's Protective Security Management Framework (Premier and Cabinet Circular 30) and Information Security Management Framework, and the agency's security management systems and practices.

Destruction or retention of personal information

Destruction or retention of the personal information must be undertaken in accordance with a disposal authority under the *State Records Act 1997*.

Expiry

This exemption is granted from 1 June 2018 to 31 May 2021. A further extension may be negotiated with the Committee if required.

Exemption – Offender Management Program

This exemption applies to the South Australia Police (SAPOL), Department for Correctional Services (DCS), Department of Human Services (DH) - formerly Department for Communities and Social Inclusion (DCSI), SA Health, Attorney-General's Department (AGD), Department of State Development (DSD), and TAFE SA. It is an exemption from compliance with IPPs 2, 8 and 10, allowing SAPOL, DCS, DCSI, AGD, DSD and TAFE SA to share case file information of serious offenders as part of the Offender Management Plan Program (OMP Program). It is an exemption from compliance with IPPs 2 and 8 allowing SA Health to share case file information of serious offenders as part of the OMP Program.

The personal information to be shared is case file information and other personal information relevant to offenders included in the OMP Program. This includes the personal information of family members and associates, where it has been identified that those individuals contribute significantly to the offending lifestyle of the nominated offender. The information is collected and held by each agency through its mandated service provision.

The purpose of the collection, use and disclosure of the personal information is to allow the successful functioning of the OMP Program in providing coordinated case management of selected serious offenders to reduce recidivism and promote community safety. This exemption also provides for the disclosure of relevant personal information to third party service providers necessary for the provision of targeted services to individual offenders under the OMP Program.

All other Principles continue to apply.

Conditions

This exemption is conditional on the following:

- personal information shared through the OMP Program is only used for the purposes of coordinated case management of selected serious offenders; and
- individual offenders are informed of their inclusion in the OMP Program; and
- the Guidelines for the OMP Program include clear pathways for complaints relating to the use of personal information; both internally and externally; and
- a system for monitoring and recording breaches of personal information privacy is maintained; and
- consent is sought from family members and associates, where it has been identified that those individuals contribute significantly to the offending lifestyle of the nominated offender, for their personal information to be shared as part of the OMP Program. Only in circumstances where consent is not granted, or if it is given and then later revoked, does this exemption apply.

Security of Personal Information

The security of the personal information should be managed in line with the Government's Protective Security Management Framework (Premier and Cabinet Circular 30) and Information Security Management Framework, and the agency's security management systems and practices. Participating agencies must specifically ensure that:

- steps taken to secure personal information are proportionate to its sensitivity and the risk of its loss or misuse;
- personal information is kept in a secure area within participating agencies;
- personal information is protected during transit;
- electronic information should be encrypted and password protected and physical files should not be left unattended in an unsecure environment; and

- access to personal information is on a strictly need-to-know basis. Personal information collected under the OMP Program should not be on-disclosed or distributed further within participating agencies for any purposes other than facilitating any actions under a participating offender's case management plan, delivering services to the offender as an existing client or where otherwise allowable under IPPs 8 and 10.

Destruction or retention of personal information

Destruction or retention of the personal information must be undertaken in accordance with a disposal authority under the *State Records Act 1997*.

Expiry

This exemption applies from 1 July 2018 to 30 June 2019.

Other Activities of the Privacy Committee

Submissions and Advice

The Privacy Committee was briefed on issues of state, national and international interest including the :

- European Union General Data Protection Regulation (GDPR)
- National Facial Biometric Matching Capability initiative
- Notifiable Data Breaches scheme under Part IIIC of the *Privacy Act 1988* (Cwth)
- Personal Information Data Breaches Guideline (SA)

Complaint Management

The Privacy Committee has within its responsibilities to refer written complaints concerning violations of individual privacy received by it (other than complaints from employees of the Crown, or agencies or instrumentalities of the Crown, in relation to their employment) to the appropriate authority.

During the reporting year the Privacy Committee referred four written complaints to state government agencies for consideration and advice.

Personal Information Data Breach Notification

To assist agencies identify and manage data breaches, a document titled Personal Information Data Breaches Guideline was developed and issued jointly by the Office for Cyber Security, Office for Data Analytics and the Privacy Committee.

During the reporting year the Privacy Committee was advised of five instances of personal information data being at risk of unauthorised access due to a breach. The Privacy Committee sought further advice and advised of areas for improvement in the management of personal information, where appropriate.