



**Government
of South Australia**

Privacy Committee of South Australia

2018-19 Annual Report

Privacy Committee of South Australia

GPO Box 464

ADELAIDE SA 50001

Enter agency website address

Contact phone number: (08) 8204 8786

Contact email: State Records

ISSN: 2208-6110

Date presented to Minister: 27 September 2019

To:

The Hon Vickie Chapman MP

Deputy Premier

Attorney-General

This annual report will be presented to Parliament to meet the statutory reporting requirements of clause 4A of the Proclamation establishing the Privacy Committee of South Australia and 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

Date 23 September 2019

Signature



From the Presiding Member

In recent years committee business has predominately related to considering exemptions from adherence with one or more of the ten information privacy principles (IPPs) within the government's *Information Privacy Principles Instruction* (IPPI) and management of complaints by individuals.

Whilst exemptions vary in complexity, an example would be a request from South Australia Police (SAPOL) for the Privacy Committee to approve conditions that allow SAPOL to use certain road crash data for analysis; to inform future policing and road safety strategy.

Following the enactment of the *Public Sector (Data Sharing) Act 2016 (Data Sharing Act)*, which provides a framework to allow for the sharing of personal information data held by state government agencies, there has been a decline in the number of exemptions sought from the Privacy Committee.

In 2018-19 there were three exemptions approved by the Privacy Committee.

Details of public sector data shared in accordance with the *Data Sharing Act* can be found on the Department for the Premier and Cabinet website.

To assist agencies deal with instances of possible or confirmed unauthorised access to personal information held by state government agencies, a policy titled *Personal Information Data Breach Guideline* was released in 2017.

The guideline requires, amongst other things, that the Privacy Committee be advised of any data breach involving personal information. During the first year of operation, 2017-18, five breaches were reported. In 2018-19 the Privacy Committee was advised of 16 breaches.

With only two years data available it is not possible to identify whether the trend for breaches is increasing. The Privacy Committee will continue to monitor the trends over the coming year and put forward recommendations for intervention as required.

Simon Froude

Presiding Member

Privacy Committee of South Australia

Contents

Overview: about the Privacy Committee	5
Committee purpose and objectives	5
Legislation (Cabinet Instruction) administered by the Committee	5
Organisation of the Committee	5
Committee Remuneration	6
Other related agencies (within the Minister’s area/s of responsibility).....	6
Privacy Committee Business	7
Exemptions from the IPPs – requested by agencies.....	7
Breaches of the IPPI – advised by agencies.....	10
Complaint Management	10

Overview: about the Privacy Committee

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.

Responsibility for the IPPI resides with the Attorney-General.

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 Privacy Committee was as follows:

Presiding Member:

- Mr Simon Froude, Director, State Records of South Australia, Attorney-General's Department – appointed to 11 January 2021.

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 2021.
- 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 2021.
- Mr Nathan Morelli, non-public sector employee – appointed to 29 January 2021.
- Ms Krystyna Slowinski, Principal Internal Auditor, Department for Communities and Social Inclusion – appointed to 1 June 2020.

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.

Other related agencies (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.

Privacy Committee Business

Exemptions from the IPPs – requested by agencies

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*'.

There were three exemptions granted during the reporting year:

Offender Management Program Accommodation Research

This exemption applies to the South Australia Police (SAPOL), Department for Correctional Services (DCS), Department of Human Services (DH), Attorney-General's Department (AGD), Department for Industry and Skills (DIS), and TAFE SA.

It is an exemption from compliance with IPPs 2, 8 and 10, allowing SAPOL, DCS, DH, AGD, DIS and TAFE SA to share case file information of high risk child sex offenders who have been participants 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 high risk child sex offenders who have been participants of the OMP Program.

The information is to be shared with the Flinders University Law School, Professor Willem de Lint and his team to enable research into best practice accommodation options for high risk child sex offenders to be undertaken. Outcomes of the research will be considered for adoption as part of the OMP Program

The personal information to be shared is case file information and other personal information of relevant OMP Program participants. 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.

All other IPPs continue to apply.

Conditions

This exemption is conditional on the following:

- Personal information of offenders held by the OMP Program that is shared with the Flinders University Law School is only used to inform research into best practice accommodation options for high risk child sex offenders; and
- Individual offenders, and where relevant their families, are informed that their personal information is to be used as part of the research project. 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.

The following specific conditions apply:

- Steps taken to secure personal information are proportionate to its sensitivity and the risk of its loss or misuse;
- All access to SAPOL electronic files will be via an onsite password protected portable storage device.
- No copies or photographs of any SAPOL data will be made of any of the information accessed; and
- Ownership of the data remains with SAPOL/OMP.

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 17 September 2018 to 30 June 2019.

School Enrolment Datasets

This exemption applies to the Department for Education and Child Development (DECD). It is an exemption from compliance with IPP 10, allowing DECD to disclose personal information to the Data Linkage Unit within SA NT Datalink.

The personal information to be disclosed is from the DECD Public Schools, including preschools, Enrolment Dataset and is limited to:

- Record Identifier
- Personal Identifier
- Names
- Date of Birth
- Sex
- Aboriginality, Torres Strait Islander Indicator
- Country of Birth
- Full address including Geocodes if available
- Parent/ Guardian Identifier
- Date Enrolled
- Date Left
- Destination School
- Census year
- Census term
- Any of the above information provided for other family members and included in these records including family code
- 85 File Number.

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 DHA 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 12 December 2015 to 31 December 2020. An extension may be negotiated with the Privacy Committee if required.

Note - exemption from 8 December 2015 is replaced by this exemption that has been amended to clarify that the term 'public schools' includes 'preschools'.

Centre for Automotive Safety

This exemption applies to the South Australia Police (SAPOL). It is an exemption from compliance with IPP 10 allowing SAPOL to disclose personal information to the Centre for Automotive Safety Research (CASR).

The personal information to be disclosed by SAPOL to CASR relates to the personal information of persons involved in vehicle collisions contained within the Vehicle Collision Report.

This information includes:

- Family and given names
- Address
- Gender
- Date of birth
- Age
- Licence number
- Licence state
- Licence status
- Phone numbers
- Seatbelt status
- Helmet status
- Hospital
- Injury level
- Breath analysis result
- BAC level
- Vehicle registration number
- Vehicle year and make
- Event Data Recorder information

The information to be disclosed is for the purpose of allowing CASR to obtain important information about collisions and to make contact with persons involved in collisions to enable CASR to gain consent to conduct in-depth interviews. Interviews greatly assist CASR to gain a better insight into vehicle accidents and to form a clearer picture of what occurred.

All other Principles continue to apply.

Conditions

This exemption is granted on the following conditions:

- Information disclosed to CASR is only to be used by CASR for the purpose of obtaining further information relevant to the research being undertaken and for contacting persons involved in vehicle collisions to gain their consent to be interviewed;
- The letter sent to persons involved in vehicle collisions for the purpose of gaining their consent explains how CASR came to be in possession of their address and other personal information; and
- CASR maintains current research ethics approvals from the University of Adelaide and SA Health.
- SAPOL 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 applies from 19 July 2018 to 18 July 2019. An extension may be negotiated with the Privacy Committee if required.

Breaches of the IPPI – advised by agencies

State government agencies are required to take particular actions in accordance with the *Personal Information Data Breach Guideline* (the Guideline) if they become aware of confirmed or potential unauthorised access to the personal information in their custody.

During the reporting year agencies notified the Privacy Committee of 16 personal information data breaches.

The Privacy Committee noted each of the breaches and where necessary sought further information or provided advice to the agency to assist them appropriately manage the breach that occurred and to reduce the likelihood of future breaches.

The majority of the breaches related to the accidental sharing of personal information held by the health and education sectors, and occurred as a result of human or system error. In each instance the agency involved took remedial action in accordance with the *Personal Information Data Breach Guideline* and there were no reports of serious effects following any of the breaches.

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 one written complaint to a state government agency for consideration and advice.