



**Government  
of South Australia**

# **PRIVACY COMMITTEE OF SOUTH AUSTRALIA**

## **2019-20 Annual Report**

Privacy Committee of South Australia

GPO Box 464

ADELAIDE SA 5001

[archives.sa.gov.au](http://archives.sa.gov.au)

Contact phone number: (08) 8204 8786

Contact email: [staterecords@sa.gov.au](mailto:staterecords@sa.gov.au)

ISSN: 2208-6110

Date presented to Minister: 30 September 2020

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 30 September 2020

Signature



## From the Presiding Member

Like many organisations, the COVID-19 pandemic impacted the operation of the Privacy Committee of South Australia (the Privacy Committee) during the second half of 2019-20. With face to face meetings unable to occur, the Privacy Committee moved to online meetings to conduct its business.

The focus of the Privacy Committee is on the operation of the Government's *Information Privacy Principles Instruction* (IPPI). Through a set of 10 information privacy principles (IPPs), the IPPI describes the ways in which state government agencies can collect, use and store the personal information in their possession.

Agencies should not collect more information than required for the associated business activity, nor should they use the information for a purpose other than the purpose for which it was collected. There are however times when it is right and proper for an agency to use the personal information they have collected to support or guide another government activity. When this need is identified agencies seek an exemption from the Privacy Committee from one or more of the IPPs.

One example is a request from the Department for Correctional Services (DCS) to approve conditions for using and disclosing personal information about inmates. DCS is able to share specified information to inform future policy development relating to inmates' health, education and justice system pathways and outcomes.

During 2019-20 the Privacy Committee approved five (5) exemptions from the IPP's.

The Government's [Personal information data breaches guideline](#) (DPC/G9.1) (the Guideline) advises agencies on how to deal with possible or confirmed unauthorised access to personal information held by state government agencies (breaches). One step within the Guideline is to notify the Privacy Committee, which then allows the Privacy Committee to work with the agency to improve privacy outcomes.

During 2019-20 the Privacy Committee received twice as many notifications than in the previous reporting year. This increase is likely due to higher awareness of the requirements of the Guideline. The Privacy Committee is pleased to see agencies identifying and implementing process improvements and educative mechanisms to mitigate the risk of future breaches.

In addition to supporting agencies and overseeing the IPPI, the Privacy Committee's representation on national privacy groups has continued. A significant focus for 2019-20 has been on ensuring policy is in place for the management of privacy through COVID-19.

Simon Froude

**Presiding Member**

**Privacy Committee of South Australia**

<b>Overview: about the Privacy Committee .....</b>	<b>5</b>
Privacy Committee's Focus and Functions.....	5
Legislation (Cabinet Instruction) administered by the Privacy Committee .....	5
Organisation of the Privacy Committee .....	6
Executive Support to the Privacy Committee.....	6
<b>Privacy Committee Business.....</b>	<b>7</b>
Exemptions from the IPPs .....	7
Agency Notification of Breaches of the IPPI .....	12
Complaint Management .....	12
Other Activities .....	12



## Overview: about the Privacy Committee

### Privacy Committee's Focus and Functions

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 Privacy 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 Privacy Committee**

Clause 1(2) of the Proclamation of the Privacy Committee establishes the membership of the Committee. It requires that the Privacy 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, Principal Consultant, Principal Consultant, SA Health Royal Commission Response Unit – appointed to 11 January 2021.
- Ms Deslie Billich, non-public sector employee – appointed to 30 January 2024.
- Ms Lucinda Byers, Special Counsel to the Crown Solicitor, Crown Solicitors Office – appointed to 30 March 2021.
- Ms Abbie Eggers, A/Manager, Disability Royal Commission, Department of Human Services – appointed until 24 January 2024.
- Mr Nathan Morelli, non-public sector employee – appointed to 29 January 2021.

## **Change of membership**

During the reporting year Ms Krystyna Slowinski's term on the Privacy Committee ended and she did not seek reappointment. Ms Slowinski, Principal Internal Auditor, Department of Human Services (DHS) was the representative of the Commissioner for Public Sector Employment and has provided outstanding service to the Privacy Committee over a six year period.

## **Executive Support to the Privacy Committee**

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 service to both agencies and the public.

## Privacy Committee Business

### Exemptions from the IPPs

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 five exemptions granted during the reporting year.

#### ***Exemption – South Australia Police - Royal Commission into Violence, Abuse, Neglect and Exploitation of People with a Disability***

This exemption applies to South Australia Police (SAPOL). It is an exemption from compliance with Principle 10, allowing the disclosure of personal information obtained by SAPOL to the Royal Commission into Violence, Abuse, Neglect and Exploitation of People with a Disability (RC) for the purpose of the RC finalising its final report addressing widespread reports of violence against, and the neglect, abuse and exploitation of people with a disability. This exemption applies to information sought by the RC outside of a 'notice to produce' or 'notice to give information' as per section 10C of the *Royal Commissions Act 1917 (Commonwealth)*.

The information to be disclosed by SAPOL to the RC relates to personal information held within SAPOL records concerning incidents of violence, abuse, neglect or exploitation of people with disabilities, such as Police Incident Reports, Apprehension Reports, statement from the victims and witnesses, offending histories, and briefs of evidence. The information to be disclosed is; family name, given name(s), current residential address, gender, age, date of birth, ethnicity, details of allegations (criminal offences)

All other Principles continue to apply.

#### Conditions

Exemption is granted on the condition that:

- Information disclosed to the RC by SAPOL is only used for the purpose of the RC discharging its responsibilities in accordance with the Letters Patent (dated 4 April 2019, amended 13 September 2019), Letters Patent with South Australia dated 20 June 2019 and with the Memorandum of Understanding (MoU) between the RC and SAPOL.
- Once transferred and disclosed, the RC will store and manage the personal information in accordance with the *Police Act 1998 (South Australia)*, the application of any claim for Public Interest Immunity, the IPPs and the *Privacy Act 1988 (Commonwealth)*. The RC undertakes to treat any information provided as law enforcement data in accordance with its obligations under clause 8 under the MoU.
- SAPOL does not disclose to the RC any details of the victims without the express consent of the victim.
- Other than where supplied in response to a summons or notice, where SAPOL discloses the information to the RC pertaining to an active investigation, the information contained within the disclosure will not be used in any hearing by the RC or made public by the RC without the express approval of SAPOL.

- Other than where supplied in response to a summons or lawful notice, any information provided by SAPOL to the RC that is classified 'Protected' or higher, will not be made public by the RC without the express approval of SAPOL.

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 South Australian Protective Security Framework and Cyber Security Framework, and the agency's security management and related or overarching Commonwealth information security policies.

#### 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 9 June 2020 to 29 April 2022. An extension may be negotiated with the Privacy Committee if required.

### ***Exemption – South Australia Police - AFL Banning Notices***

This exemption applies to South Australia Police (SAPOL). It is an exemption from compliance with Principle 10, allowing the disclosure of personal information obtained by an on duty member of SAPOL at National Australian Football League (AFL) matches to an authorised AFL officer (AFLO) for the purpose of the AFLO issuing an AFL Banning Notice.

The personal information to be disclosed by SAPOL to an AFLO relates to patrons who have been arrested, reported and/or evicted from an AFL match by an on duty member of SAPOL. The information to be disclosed is; family name, given name(s), current residential address, date of birth, photograph (if taken)

All other Principles continue to apply.

#### Conditions

Exemption is granted on the condition that information disclosed to the AFL by SAPOL is only used for the purpose of issuing of a banning notice.

Exemption is granted on the condition that once transferred and disclosed, the AFL will store the personal information in its secured Incident Management System (IMS) and that the information will only be accessed by members of the AFL Integrity and Security Department.

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.

#### 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 February 2020 to 30 September 2020. An extension may be negotiated with the Privacy Committee if required.

### ***Exemption – Wellbeing SA and the Commission on Excellence and Innovation in Health***

This exemption applies to Wellbeing SA (WBSA) and the Commission on Excellence and Innovation in Health (CEIH). It is an exemption from compliance with parts of the IPPs, only to the extent that the IPPs conflict with the Ministerial Direction (the Direction) issued by the Minister for Health and Wellbeing on 21 December 2019.

The Direction, to staff, officers or employees of WBSA and CEIH in relation to the disclosure of personal information specifically states that staff, officers and employees of these attached offices established under section 27 of the *Public Sector Act 2009*, effective 6 January 2020:

MUST NOT disclose personal information relating to a person obtained in the course of, or in connection with, their role and duties within these attached offices;

EXCEPT in the following circumstances:

- A to the extent that he or she may be authorised or required to disclose that information by the Minister for Health and Wellbeing, or any person with delegated authority of the Minister ("the Minister's delegate"); or
- B as required or authorised by or under law; or
- C at the request, or with the consent, of –
  - i. the person to whom the information relates; or
  - ii. a guardian of the person to whom the information relates; or
  - iii. a medical agent of the person to whom the information relates; or
  - iv. a substitute decision-maker for the person to whom the information relates (within the meaning of the *Advance Care Directives Act 2013*); or
- D to a relative, carer or friend of the person to whom the information relates if –
  - i. the disclosure is reasonably required for the treatment, care or rehabilitation of the person; and
  - ii. there is no reason to believe that the disclosure would be contrary to the person's best interests; or
- E to a health or other service provider if the disclosure is reasonably required for the treatment, care or rehabilitation of the person to whom the information relates; or
- F disclosing information by entering the information into an electronic records system established for the purpose of enabling the recording or sharing of information between persons or bodies involved in the provision of health services; or
- G disclosing the information to such extent as is reasonably required in connection with the management or administration of an incorporated hospital under the *Health Care Act 2008* or SA Ambulance Service (including for the purposes of charging for a service); or

- H disclosing information if the disclosure is reasonably required to lessen or prevent a serious threat to the life, health or safety of a person, or a serious threat to public health or safety; or
- I disclosing information for medical or social research purposes if the research methodology had been approved by an ethics committee and there is no reason to believe that the disclosure would be contrary to the person's best interests; or
- J disclosing information in accordance with the *Health Care Regulations* 2008 (where applicable).

Conditions of the Direction:

1. Personal information must not be disclosed to a relative, carer or friend of the person to whom the information relates (in accordance with point (D) above) in contravention of a direction given by the person to whom the information relates.
2. Personal information must not be disclosed under this Direction unless an exemption such as this exemption is in place to address conflicts 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), the SA Protective Security Framework, and the agency's security management.

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 6 January 2020 to 5 January 2021. An extension may be negotiated with the Privacy Committee if required.

***Exemption – Department for Correctional Services – SA NT Data linkage***

This exemption applies to the Department for Correctional Services (DCS). It is an exemption from compliance with Principle 10, allowing DCS to disclose personal information to the Data Linkage Unit within SA NT DataLink.

The personal information to be disclosed by DCS relates to individuals who have been sentenced to a period of supervision, either in a custodial setting or in the community and is limited to; DCS IDs, JIS PIN, entry and exit dates, surnames (including previous names and maiden names), given name(s) (all including "aka's", aliases and nicknames), date of birth, sex, residential address and postcodes (including previous addresses), Aboriginal and Torres Strait Islander indicator.

The information to be disclosed will enable researchers and policy analysts to develop and disseminate a more comprehensive understanding of health, education and justice system pathways and outcomes.

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.

DCS 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 5 December 2019 to 31 December 2020. An extension may be negotiated with the Privacy Committee if required.

***Exemption extension – SA Housing Authority – SA NT Data linkage - Homeless to Home Data***

This exemption applies to the SA Housing Authority (SAHA), formally a business unit within the Department for Communities and Social Inclusion. It is an exemption from compliance with Principle 10, allowing the SAHA to disclose personal information to the Data Linkage Unit within SA NT DataLink.

The personal information to be disclosed is from the SAHA Homelessness to Home (H2H) data set and is limited to; H2H customer number, Housing SA customer number, given names, surname, date of birth, sex, Aboriginality and/or Torres Strait Islander indicator, country of birth, full address details (including past addresses where available), system date, any of the above information provided for other family members and included in these records

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.

SAHA 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 17 August 2019 to 31 December 2020. A further extension may be negotiated with the Privacy Committee if required.

## **Agency Notification of Breaches of the IPPI**

State government agencies are required to take particular actions in accordance with the [Personal information data breaches guideline](#) (DPC/G9.1) (the Guideline) if they become aware of confirmed or potential unauthorised access to the personal information in their custody. The Guideline was released in 2017.

During the reporting year agencies notified the Privacy Committee of 33 personal information data breaches. This is twice as many notifications than in the previous reporting year. The increase is likely due to higher awareness of the requirements of the Guideline.

Where necessary the Privacy Committee sought further information or provided advice to the agency to assist them to 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 staff within the health sector, and occurred as a result of human or system error. In each instance the agency took remedial action in accordance with the Guideline and there were no reports of serious effects following any of the breaches.

## **Complaint Management**

The Privacy Committee has within its responsibilities the referral of 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 seven written complaints to state government agencies for consideration and advice.

## **Other Activities**

### National group representation

The Privacy Committee is represented by the Presiding Member and senior staff from within State Records on a number of national groups including:

Privacy Authorities Australia

Privacy Authorities Australia – Policy Group and Complaints and Compliance Group

National COVID-19 Privacy Team

### Support to State Government agencies

Tools and other guidance materials are developed and maintained to support state government meet their obligations under the IPPI. During the reporting year a draft Privacy Impact Assessment template and other guidance materials were developed. The Presiding Member also provided privacy input to deliberations relating to future government service delivery.