Privacy Management Plan

Sport Integrity Australia

1 July 2022 to 30 June 2023

Background

What is a Privacy Management Plan?

A Privacy Management Plan (**PMP**) is a document that identifies specific, measurable privacy goals and targets and sets out how an agency will meet its compliance obligations under APP 1.2. An agency must measure and document its performance against its privacy management plan at least annually.

Before developing a PMP, every agency will need to understand the current state of their privacy practices. Agencies should refer to the OAIC's *Interactive PMP Explained* resource for guidance on how to identify compliance gaps and opportunities to improve maturity.

What are the next steps?

This PMP describes the actions that the agency must take in order to meet its privacy compliance obligations and and maturity targets for the year following the PMP's commencement date (specified below). The agency must take steps to achieve these actions and to record how it has done so.

This PMP should be kept up to date over the course of the year. In the recommended review period (specified below), the agency should return to this PMP and use it to assess how well it agency has met and delivered its privacy targets.

The agency should start the review process early enough to develop a strong PMP that can be endorsed by management and put into place by the start of the next year (for example, on 1 July). By completing this process in a timely way, the agency will be best placed to highlight priority activities for the coming year to senior management and seek the resources it will need to undertake them.

About this PMP

Agency name	Sport Integrity Australia
PMP commencement date	Friday, 1 July 2022
PMP end date	Following commencement, this PMP will operate until Friday, 30 June 2023.
Recommended review period	Saturday, 1 April 2023 to Friday, 30 June 2023
PMP review date	A review date has not been provided.

Privacy risk profile

In the course of preparing this PMP, the agency has considered various matters relevant to its privacy risk profile. The details of these considerations are provided below for reference.

Privacy risk profile rationale	HIGH RISK. Sport Integrity Australia (SIA) is a regulatory agency that collects personal information to carry out

Current state

Privacy maturity assessment outcomes

This PMP has been prepared using an assessment of the agency's privacy maturity, the results of which are recorded in the table below. An asterisk (*) next to an attribute name means that it it a 'compliance attribute' and that your agency must have a minimum maturity level of 'Developing' to comply with the Privacy Act or the Code.

Governance & Culture			
Attribute	**Current Level**	**Target Level**	**Rationale/Commentary**
Privacy Champion*	**Developing**	**Defined**	A Privacy Champion has been designated. The Chief Operations Officer (COO) (SES1) has responsiblility for privacy across the agency, however, this appointment needs to be documented in policy and procedures.

Privacy Values	**Developing**	**Defined**	There is a connection between the agency's values and respecting and protecting personal information and staff understand this connection. Staff have general awareness of privacy obligations and secrecy provisions as contained in the SIA Act.
Privacy Officer*	**Developing**	**Defined**	A Privacy Officer has been designated. The Privacy Officer is an EL1 in the Legal Team. This appointment needs to be formally documented in policy and procedures.
Management & Accountability	**Developing**	**Defined**	The agency has assigned responsibility for privacy compliance including senior oversight and operations. The Privacy Champion oversees privacy within the agency, and the Legal team manages privacy issues on a day-to-day basis (i.e. breaches). Roles and acountabilities for privacy compliance and oversight need to be documented and further understood across the agency.
Awareness	**Developing**	**Defined**	Staff have a general understanding of privacy obligations and secrecy provisions under the SIA Act. Further training, including on induction, is required.
Element score (average of attribute scores)			**2 / 4 (Developing)**

Privacy Strategy			
Attribute	**Current Level**	**Target Level**	**Rationale/Commentary**
Privacy Management Plan*	**Initial**	**Defined**	s 47C, s 47E(d) [redacted]

Inventory of Personal Information*	Initial	Defined	Broad bategorites of personal information SIA collects are described in the Privacy Policy. s 47C, s 47E(d) .
Data Quality Processes*			
Information Security Processes	Defined	Defined	SIA has an established information-security aware culture. Staff understand the commonalities and differences between privacy and security and are aware of relevant privacy and security policies and processes.
Element score (average of attribute scores)			

Privacy Processes			
Attribute	Current Level	Target Level	Rationale/Commentary
External Privacy Policy & Notices*			
Internal Policies & Procedures			
Privacy Training*			
Privacy Impact Assessments*			
Dealing with Suppliers			
Access & Correction*			
Complaints & Enquiries			
Element score (average of attribute scores)			

Risk & Assurance			
Attribute	Current Level	Target Level	Rationale/Commentary
Risk Identification & Assessment			
Reporting & Escalation			
Assurance Model			
Element score (average of attribute scores)			

Data Breach Response			
Attribute	**Current Level**	**Target Level**	**Rationale/Commentary**
Data Breach Response Plan			
Data Breach Notification*			
Element score (average of attribute scores)			

Average of element scores	
Overall privacy maturity level	

Adequacy of privacy policy and notices

Section 17 of the Code requires an agency to regularly assess the adequacy of its privacy practices, procedures and systems (including its privacy policy and collection notices) to ensure their adequacy for the purpose of compliance with the APPs and currency. Generally, completion of a PMP facilitates compliance with this requirement.

The outcomes of the agency's review of its privacy policy and collection notices are recorded below.

Privacy Policy (APP 1) Compliance Gaps	No gaps provided in Step 1
Privacy Policy (APP 1) Currency Gaps	No gaps provided in Step 1
Privacy Notices (APP 5) Compliance Gaps	No gaps provided in Step 1
Privacy Notices (APP 5) Currency Gaps	No gaps provided in Step 1

Goals for improvement

The privacy goals and targets in this section are based on the agency's privacy maturity assessment outcomes. This section includes mandatory actions which the agency must take in order to meet its compliance obligations under APP 1.2 (Code, s 9(2)(b)).

Compliance Actions

Where the agency has identified in its privacy maturity assessment that it is at the 'Initial' level in relation to a compliance attribute, this indicates that there is a compliance gap because the agency must have a minimum maturity level of 'Developing' for that attribute in order to comply with the Privacy Act or the Code. All compliance gaps must form part of this PMP and may require prompt remediation. Remediation actions are set out below.

Attribute	Remediation action	Responsible person, position or team	Due	Required resources, dependencies and/or related documents (specify or link)
There are no compliance actions defined in this PMP.				

Privacy Policy & Notices Actions

Remediation actions related to any gaps in the adequacy of the agency's Privacy Policy (APP 1) or Privacy Notices (APP 5) are captured below.

Attribute	Remediation actions	Responsible person, position or team	Due	Required resources, dependencies and/or related documents (specify or link)
There are no privacy policy & notices actions defined in this PMP.				

Maturity Improvement Actions

The table below sets out actions which the agency plants to achieve in order to improve its privacy maturity. Any uncompleted actions from previous PMPs which are still relevant should also be documented in this section to ensure that they form part of the agency's next PMP.

Element / Attribute	Action	Responsible person, position or team	Due	Required resources, dependencies and/or related documents (specify or link)
There are no privacy maturity improvement actions defined in this PMP.				

Bringing the PMP together and prioritising actions

This section of the PMP identified all compliance actions and actions for improvement, as well as who is responsible for delivery of each action, interdependencies and due dates. From here, prioritisation is a key part of establishing an achievable PMP. Agencies should take a risk-based approach to prioritising and timing their improvement activities.

Measure performance

It is expected that the agency will review this PMP during the time in which it is active in order to document progress against the actions described above.

The table below provides a central location to track progress.

Action	Achieved	Future actions / commentary
There are no actions defined in this PMP.		

Privacy Management Plan

Sport Integrity Australia

1 September 2022 to 31 August 2023

Background

What is a Privacy Management Plan?

A Privacy Management Plan (**PMP**) is a document that identifies specific, measurable privacy goals and targets and sets out how an agency will meet its compliance obligations under APP 1.2. An agency must measure and document its performance against its privacy management plan at least annually.

Before developing a PMP, every agency will need to understand the current state of their privacy practices. Agencies should refer to the OAIC's *Interactive PMP Explained* resource for guidance on how to identify compliance gaps and opportunities to improve maturity.

What are the next steps?

This PMP describes the actions that the agency must take in order to meet its privacy compliance obligations and and maturity targets for the year following the PMP's commencement date (specified below). The agency must take steps to achieve these actions and to record how it has done so.

This PMP should be kept up to date over the course of the year. In the recommended review period (specified below), the agency should return to this PMP and use it to assess how well it agency has met and delivered its privacy targets.

The agency should start the review process early enough to develop a strong PMP that can be endorsed by management and put into place by the start of the next year (for example, on 1 July). By completing this process in a timely way, the agency will be best placed to highlight priority activities for the coming year to senior management and seek the resources it will need to undertake them.

About this PMP

Agency name	Sport Integrity Australia
PMP commencement date	Thursday, 1 September 2022
PMP end date	Following commencement, this PMP will operate until Thursday, 31 August 2023.
Recommended review period	Thursday, 1 June 2023 to Thursday, 31 August 2023
PMP review date	A review date has not been provided.

Privacy risk profile

In the course of preparing this PMP, the agency has considered various matters relevant to its privacy risk profile. The details of these considerations are provided below for reference.

Privacy risk profile rationale	High risk. The agency handles a broad range of personal information in connection with its functions and activities, including 'sensitive information' and 'health information' of individuals.

Current state

Privacy maturity assessment outcomes

This PMP has been prepared using an assessment of the agency's privacy maturity, the results of which are recorded in the table below. An asterisk (*) next to an attribute name means that it it a 'compliance attribute' and that your agency must have a minimum maturity level of 'Developing' to comply with the Privacy Act or the Code.

Governance & Culture			
Attribute	**Current Level**	**Target Level**	**Rationale/Commentary**

Privacy Champion*	**Developing**	**Defined**	A Privacy Champion has been designated. The Chief Operations Officer (COO) (SES1) has responsibility for privacy across the agency. This appointment will be documented in internal policies and procedures, including how the role operates in promoting awareness and reporting to and informing the agency leadership on privacy-related matters.
Privacy Values	**Developing**	**Defined**	There is a connection between the agency's values and respecting and protecting personal information, and staff understand this connection. Staff have general awareness of privacy obligations and secrecy provisions as contained in the SIA Act.
Privacy Officer*	**Developing**	**Defined**	A Privacy Officer has been designated. The Privacy Officer is an EL1 in the Legal Team, and duties may be shared with other staff within the Legal Team when required. The role of the privacy officer will be reflected in agency policies and procedures, including a privacy manual. Contact details have been provided to the OAIC.
Management & Accountability	**Developing**	**Defined**	The agency has assigned responsibility for privacy compliance including senior oversight and operations. The Privacy Champion oversees privacy within the agency, and the Privacy Officer and Legal Team manage privacy issues on a day-to-day basis (e.g. handling complaints and data breaches and providing advice to business areas). Roles and acountabilities for privacy compliance and oversight could be documented and further understood across the agency, and embedded as part of Executive reporting.
Awareness	**Developing**	**Defined**	Staff have a general understanding of privacy obligations and secrecy provisions under the SIA Act. Whole of agency privacy training will occur in 2022, and for new staff upon induction.
Element score (average of attribute scores)			**2 / 4 (Developing)**

Privacy Strategy			
Attribute	**Current Level**	**Target Level**	**Rationale/Commentary**
Privacy Management Plan*	**Developing**	**Defined**	The agency will have a privacy management plan (PMP) in place in 2022. This PMP will be used to track and report on agency compliance and progress against the privacy maturity model to agency leadership bi-annually. For the agency to move from 'Developing' to 'Defined' in the privacy maturity model, the agency should have the PMP endorsed by senior management so that they are made aware of the PMP and the agency's objectives under it.
Inventory of Personal Information*	**Developing**	**Defined**	The agency is developing its inventory of personal information in the form of a register of personal information holdings. A template for reporting on holdings has been developed and disributed to line areas, and responses provided. A completed register will be in place in 2022.
Data Quality Processes*	**Developing**	**Defined**	The agency is starting to define processes to monitor and improve the quality of personal information. Development of privacy resources, and privacy training in 2022 will increase staff awareness of the requirements to ensure that the personal information the agency handles is accurate, up-to-date, complete and relevant. As part of the review of SIA's personal information holdings, the agency will consider whether further guidance in relation to records management is needed.
Information Security Processes	**Developing**	**Defined**	The agency operates within a 'Protected' environment. Staff receive regular training on ICT security including measures such as appropriate use of passes, password security, avoiding spam and phishing emails, and other protective measures. Privacy training in 2022 will increase staff awareness of the requirements of APP11 and of the notifiable data breaches scheme.
Element score (average of attribute scores)			**2 / 4 (Developing)**

Privacy Processes			
Attribute	**Current Level**	**Target Level**	**Rationale/Commentary**
External Privacy Policy & Notices*	**Developing**	**Defined**	The agency privacy policy is available to the public via the agency website. The privacy policy will be reviewed in 2022 to ensure that it is up to date, user friendly, expressed in plain english, transparent and legally compliant. Updated template long form and short form privacy collection notice templates will be made available to all staff in 2022.
Internal Policies & Procedures	**Developing**	**Defined**	There are existing procedures within the agency that have privacy enhancing elements, s 47C, s 47E(d) [redacted] The agency is in the process of reviewing its policies and procedures and will have a privacy manual, privacy fact sheet and other complementary resources in place by the end of 2022. Updated policies and procedures will be communicated to staff to make sure they are understood and followed.
Privacy Training*	**Developing**	**Defined**	Al staff will attend privacy training in 2022. Privacy materials will be completed in 2022 to support the education and training of any new staff or contractors upon induction.
Privacy Impact Assessments*	**Developing**	**Defined**	The agency is aware of its obligations to undertake PIAs where a project is 'high risk'. The agency has a Privacy Impact Assessment Register published on its website. s 47C, s 47E(d) [redacted] The agency will develop its own or utilise the OAIC's Privacy Threshold Assessment template to assist it to identify whether PIAs are necessary. The agency will highlight the requirement for and benefits of undertaking PIAs as part of all staff privacy training in 2022.

Dealing with Suppliers	**Developing**	**Defined**	The agency is reviewing its processes to ensure that all contracts entered into on behalf of the agency incorporate appropriate privacy and confidentiality terms, as required by s 95B of the Privacy Act.
Access & Correction*	**Developing**	**Defined**	The privacy officer is responsible for handling any requests for access or correction, which are infrequent. The agency privacy policy sets out how to request access and correction, and provides a privacy email address for this purpose. The agency has procedures for the management of and response to requests for access and correction. The agency will document these procedures in its Privacy Manual, to be completed by end of 2022.
Complaints & Enquiries	**Developing**	**Defined**	The privacy officer is responsible for handling any privacy complaints, which are infrequent. The agency privacy policy sets out how to make a complaint, and provides a privacy email address for this purpose. The agency has procedures for responding to complaints and enquiries. The agency will document these procedures in its Privacy Manual, to be completed by end of 2022.
Element score (average of attribute scores)			**2 / 4 (Developing)**

Risk & Assurance			
Attribute	**Current Level**	**Target Level**	**Rationale/Commentary**
Risk Identification & Assessment	**Developing**	**Defined**	The agency identifies privacy risks using available resources and legal support where required. The development of key privacy governance resources and rollout of training in 2022 will enhance the agency's ability to identify, assess and deal with privacy risks.

Reporting & Escalation	**Initial**	**Defined**	The agency is responsive to incidents, and escalates and reports to senior leadership on an ad hoc basis. Measures to formalise reporting and escalation of privacy incidents will be considered and developed in 2022 as part of a review of key privacy governance documents (e.g. the finalisation of a Data Breach Response Plan, and considering the role of Privacy Champion in reporting regularly to senior leaderhip on privacy related matters).
Assurance Model	**Initial**	**Defined**	First and second line assurance privacy controls are in place through the established functions of the Privacy Officer and Privacy Champion. s 47C, s 47E(d) [redacted]
Element score (average of attribute scores)			**1.3 / 4 (Initial)**

Data Breach Response			
Attribute	**Current Level**	**Target Level**	**Rationale/Commentary**
Data Breach Response Plan	**Initial**	**Defined**	A data breach response plan is being finalised as part of the review of privacy governance documents, and a formal plan will be in place in 2022. Efforts have been made to improve awareness of how to identify and respond to data breaches.

Data Breach Notification*	**Developing**	**Defined**	Data breaches can be reported to the privacy officer. s 47C, s 47E(d) [redacted]. The privacy officer is responsible for notifying the OAIC and individuals. Data breach identification, assessment, mitigation and notification will be addressed in whole of agency privacy training in 2022.
Element score (average of attribute scores)			**1.5 / 4 (Initial)**

Average of element scores	**1.8 / 4**
Overall privacy maturity level	**2 / 4 (Developing)**

Adequacy of privacy policy and notices

Section 17 of the Code requires an agency to regularly assess the adequacy of its privacy practices, procedures and systems (including its privacy policy and collection notices) to ensure their adequacy for the purpose of compliance with the APPs and currency. Generally, completion of a PMP facilitates compliance with this requirement.

The outcomes of the agency's review of its privacy policy and collection notices are recorded below.

Privacy Policy (APP 1) Compliance Gaps	Privacy Policy is in place, and will be be reviewed in 2022 to check compliance.
Privacy Policy (APP 1) Currency Gaps	Privacy Policy to be updated to ensure it reflects all of the agency's functions and activities, and all types of personal information collected.
Privacy Notices (APP 5) Compliance Gaps	General template notices to be developed in 2022. Athletes Privacy Statement is in place.
Privacy Notices (APP 5) Currency Gaps	General template notices to be developed in 2022. Athletes Privacy Statement is in place.

Goals for improvement

The privacy goals and targets in this section are based on the agency's privacy maturity assessment outcomes. This section includes mandatory actions which the agency must take in order to meet its compliance obligations under APP 1.2 (Code, s 9(2)(b)).

Compliance Actions

Where the agency has identified in its privacy maturity assessment that it is at the 'Initial' level in relation to a compliance attribute, this indicates that there is a compliance gap because the agency must have a minimum maturity level of 'Developing' for that attribute in order to comply with the Privacy Act or the Code. All compliance gaps must form part of this PMP and may require prompt remediation. Remediation actions are set out below.

Attribute	Remediation action	Responsible person, position or team	Due	Required resources, dependencies and/or related documents (specify or link)
There are no compliance actions defined in this PMP.				

Privacy Policy & Notices Actions

Remediation actions related to any gaps in the adequacy of the agency's Privacy Policy (APP 1) or Privacy Notices (APP 5) are captured below.

Attribute	Remediation actions	Responsible person, position or team	Due	Required resources, dependencies and/or related documents (specify or link)
Privacy Policy (APP 1)	Reviewing privacy policy to ensure it is up-to-date, and reflects the functions and activities of the agency, and the types of collections that may occur.	Privacy Officer, Legal Team	1/12/2022	

Privacy Notices (APP 5)	Athletes Statement is in place. Agency is preparing template privacy notices to be utilised by business areas when collecting personal information.	Privacy Officer, Legal Team	1/12/2022	

Maturity Improvement Actions

The table below sets out actions which the agency plants to achieve in order to improve its privacy maturity. Any uncompleted actions from previous PMPs which are still relevant should also be documented in this section to ensure that they form part of the agency's next PMP.

Element / Attribute	Action	Responsible person, position or team	Due	Required resources, dependencies and/or related documents (specify or link)

Governance & Culture / Privacy Champion	Privacy Officer to work with Privacy Champion to promote a culture of privacy that values and protects personal information, and supports the integration of privacy practices, procedures and systems into broader organisational frameworks. Privacy awareness raising activities to occur in privacy awareness week and throughout the year. s 47C, s 47E(d) Privacy Champion to report regularly to senior leadership.	Privacy Officer Privacy Champion		
Governance & Culture / Privacy Values	Privacy governance documents to be developed and distributed to staff (possibly via a dedicated intranet page). Privacy training in 2022 will emphasise the importance of privacy as a core value that is central to the reputation of the agency.	Privacy Officer & ICT		

Governance & Culture / Privacy Officer	The designated Privacy Officer will establish practices, procedures and systems to support their obligations. These will be documented as part of a privacy governance review by end of 2022. Reporting frameworks will be considered to embed broader privacy awareness for senior leadership and across the agency. Privacy training will occur in 2022 will build awareness of the role of the Privacy Officer and enable broader privacy compliance.	Privacy Officer Privacy Champion		
Governance & Culture / Management & Accountability	Privacy Management Plan and key privacy policies and procedural documents to be approved by senior leadership, and annual review and approval to be scheduled. Execeutive reporting will be considered to ensure visibility of high risk privacy issues, and to assist the agency to track activity against this PMP.	Privacy Officer Privacy Champion		

Governance & Culture / Awareness	Changes to policies and procedures will be distributed to staff. Privacy training will be provided to all staff in 2022.	Privacy Officer		
Privacy Strategy / Privacy Management Plan	PMP will be endorsed by Executive in 2022, and implemented by the Privacy Officer and Privacy Champion. Privacy Officer and Privacy Champion will consider options s 47C, s 47E(d) [redacted]	Privacy Officer Privacy Champion Executive		
Privacy Strategy / Inventory of Personal Information	Register of Personal Information Holdings will be endorsed by Executive, and procedures developed for it to be reviewed on an annual basis. Template emails to inform the register will be provided to business areas when there is a change of structure, or at each review point.	Privacy Officer Executive		

Privacy Strategy / Data Quality Processes	Privacy documents, including the privacy manual and privacy fact sheet, will be disributed to staff to inform them of the need to maintain quality of personal information. All staff training in 2022 will embed understanding by agency personnel of obligations with respect to the quality of personal information.	Privacy Officer		

Privacy Strategy / Information Security Processes	The agency has existing policies in respect of securing its premises and information holdings, and staff are aware of this. Procedural documents, such as the privacy manual and factsheet, set out relevant information, and provide links to other resources to assist staff in securing personal information. A data breach response plan will be endorsed in 2022, and will assist staff to understand their obligations in relation to preventing and mitigating data breaches. Further consideration will be given to other measures that may be taken to boost protection of personal information.	Privacy Officer ICT		
Privacy Processes / External Privacy Policy & Notices	Privacy Policy is being reviewed and will be endorsed in 2022. Privacy notice templates are being developed and will be endorsed in 2022.	Privacy Officer		
Privacy Processes / Internal Policies & Procedures	A comprehensive privacy governance review is underway, and policies and procedures will be in place in 2022.	Privacy Officer		

Privacy Processes / Privacy Training	Privacy training materials are being developed and finalised in 2022. All agency privacy training will take place in 2022, and then on an annual basis, and for new personnel upon induction.	Privacy Officer		
Privacy Processes / Privacy Impact Assessments	The privacy manual and fact sheet (to be endorsed in 2022) will set out requirements for the conduct of PIAs. Consideration will be given to any additional resources/templates that may be required. OAIC resources will be leveraged and referred to in the privacy manual. All agency privacy training in 2022 will emphasise the requirement for PIAs for all high risk privacy projects involving new or changed ways of handling personal information.	Privacy Officer		

Privacy Processes / Dealing with Suppliers	Privacy Officer to review agency processes for assessing third party contracts to ensure privacy requirements are met.	Privacy Officer		
Privacy Processes / Access & Correction	Privacy manual will be put in place by end of 2022 that addresses process for action and correction. Privacy training for all staff in 2022 will address access and correction.	Privacy Officer		
Privacy Processes / Complaints & Enquiries	Privacy manual will incorporate processes for dealing with privacy enquiries and complaints. All agency privacy training in 2022 will empower staff to respond appropriately to enquiries and complaints.	Privacy Officer		

Risk & Assurance / Risk Identification & Assessment	Privacy governance review will ensure strong, clear and consistent processes that will aid agency staff to identify and assess privacy risks. Privacy Officer and Privacy Champion will manage risks, and make these visible to Executive through regular reporting.	Privacy Officer		
Risk & Assurance / Reporting & Escalation	Privacy Officer and Privacy Champion to consider options for executive reporting and incident escalation. Privacy Officer and Privacy Champion to consider integrating privacy into broader risk management and planning processes.	Privacy Officer		

Risk & Assurance / Assurance Model	Privacy Officer and Privacy Champion to consider options for executive reporting and incident escalation. Privacy Officer and Privacy Champion to consider integrating privacy into broader risk management and planning processes. Privacy officer to engage with ICT to form a strong mutual understanding of IT/privacy related risks. Privacy officer to consider whether there are assurance methods that might be developed.	Privacy Officer		
Data Breach Response / Data Breach Response Plan	Comprehensive data breach response plan will be endorsed by end of 2022. All agency training in 2022 will educate staff on how to identify, contain and escalate data breaches. Agency to develop process for reporting data breaches to Executive.	Privacy Officer		

Data Breach Response / Data Breach Notification	Data breach response plan addresses notification requirements. Privacy Officer will have responsibility for notifying breaches, and will seek legal advice where necessary.	Privacy Officer		
Governance & Culture / Privacy Champion	s 47C, s 47E(d)	Privacy Champion & Executive		
Governance & Culture / Privacy Officer	s 47C, s 47E(d)	Privacy Officer, Privacy Champion & Executive		

Bringing the PMP together and prioritising actions

This section of the PMP identified all compliance actions and actions for improvement, as well as who is responsible for delivery of each action, interdependencies and due dates. From here, prioritisation is a key part of establishing an achievable PMP. Agencies should take a risk-based approach to prioritising and timing their improvement activities.

Measure performance

It is expected that the agency will review this PMP during the time in which it is active in order to document progress against the actions described above.

The table below provides a central location to track progress.

Action	Achieved	Future actions / commentary
Reviewing privacy policy to ensure it is up-to-date, and reflects the functions and activities of the agency, and the types of collections that may occur.		
Athletes Statement is in place. Agency is preparing template privacy notices to be utilised by business areas when collecting personal information.		

Privacy Officer to work with Privacy Champion to promote a culture of privacy that values and protects personal information, and supports the integration of privacy practices, procedures and systems into broader organisational frameworks. Privacy awareness raising activities to occur in privacy awareness week and throughout the year. s 47C, s 47E(d) Privacy Champion to report regularly to senior leadership.		
Privacy governance documents to be developed and distributed to staff (possibly via a dedicated intranet page). Privacy training in 2022 will emphasise the importance of privacy as a core value that is central to the reputation of the agency.		
The designated Privacy Officer will establish practices, procedures and systems to support their obligations. These will be documented as part of a privacy governance review by end of 2022. Reporting frameworks will be considered to embed broader privacy awareness for senior leadership and across the agency. Privacy training will occur in 2022 will build awareness of the role of the Privacy Officer and enable broader privacy compliance		

Privacy Management Plan and key privacy policies and procedural documents to be approved by senior leadership, and annual review and approval to be scheduled. Execeutive reporting will be considered to ensure visibility of high risk privacy issues, and to assist the agency to track activity against this PMP.		
Changes to policies and procedures will be distributed to staff. Privacy training will be provided to all staff in 2022.		
PMP will be endorsed by Executive in 2022, and implemented by the Privacy Officer and Privacy Champion. Privacy Officer and Privacy Champion will consider options for ensuring the PMP and privacy considerations are planned for in the budgeting process.		
Register of Personal Information Holdings will be endorsed by Executive, and procedures developed for it to be reviewed on an annual basis. Template emails to inform the register will be provided to business areas when there is a change of structure, or at each review point.		

Privacy documents, including the privacy manual and privacy fact sheet, will be disributed to staff to inform them of the need to maintain quality of personal information. All staff training in 2022 will embed understanding by agency personnel of obligations with respect to the quality of personal information.		
The agency has existing policies in respect of securing its premises and information holdings, and staff are aware of this. Procedural documents, such as the privacy manual and factsheet, set out relevant information, and provide links to other resources to assist staff in securing personal information. A data breach response plan will be endorsed in 2022, and will assist staff to understand their obligations in relation to preventing and mitigating data breaches. Further consideration will be given to other measures that may be taken to boost protection of personal information.		
Privacy Policy is being reviewed and will be endorsed in 2022. Privacy notice templates are being developed and will be endorsed in 2022.		
A comprehensive privacy governance review is underway, and policies and procedures will be in place in 2022.		

Privacy training materials are being developed and finalised in 2022. All agency privacy training will take place in 2022, and then on an annual basis, and for new personnel upon induction.		
The privacy manual and fact sheet (to be endorsed in 2022) will set out requirements for the conduct of PIAs. Consideration will be given to any additional resources/templates that may be required. OAIC resources will be leveraged and referred to in the privacy manual. All agency privacy training in 2022 will emphasise the requirement for PIAs for all high risk privacy projects involving new or changed ways of handling personal information.		
Privacy Officer to review agency processes for assessing third party contracts to ensure privacy requirements are met.		

Privacy manual will be put in place by end of 2022 that addresses process for action and correction. Privacy training for all staff in 2022 will address access and correction.		
Privacy manual will incorporate processes for dealing with privacy enquiries and complaints. All agency privacy training in 2022 will empower staff to respond appropriately to enquiries and complaints.		
Privacy governance review will ensure strong, clear and consistent processes that will aid agency staff to identify and assess privacy risks. Privacy Officer and Privacy Champion will manage risks, and make these visible to Executive through regular reporting.		
Privacy Officer and Privacy Champion to consider options for executive reporting and incident escalation. Privacy Officer and Privacy Champion to consider integrating privacy into broader risk management and planning processes.		

Privacy Officer and Privacy Champion to consider options for executive reporting and incident escalation. Privacy Officer and Privacy Champion to consider integrating privacy into broader risk management and planning processes. Privacy officer to engage with ICT to form a strong mutual understanding of IT/privacy related risks. Privacy officer to consider whether there are assurance methods that might be developed.		
Comprehensive data breach response plan will be endorsed by end of 2022. All agency training in 2022 will educate staff on how to identify, contain and escalate data breaches. Agency to develop process for reporting data breaches to Executive.		
Data breach response plan addresses notification requirements. Privacy Officer will have responsibility for notifying breaches, and will seek legal advice where necessary.		
s 47C, s 47E(d) s 47C, s 47E(d)		

Privacy Management Plan

Sport Integrity Australia

29 March 2023 to 28 March 2024

Background

What is a Privacy Management Plan?

A Privacy Management Plan (**PMP**) is a document that identifies specific, measurable privacy goals and targets and sets out how an agency will meet its compliance obligations under APP 1.2. An agency must measure and document its performance against its privacy management plan at least annually.

Before developing a PMP, every agency will need to understand the current state of their privacy practices. Agencies should refer to the OAIC's *Interactive PMP Explained* resource for guidance on how to identify compliance gaps and opportunities to improve maturity.

What are the next steps?

This PMP describes the actions that the agency must take in order to meet its privacy compliance obligations and and maturity targets for the year following the PMP's commencement date (specified below). The agency must take steps to achieve these actions and to record how it has done so.

This PMP should be kept up to date over the course of the year. In the recommended review period (specified below), the agency should return to this PMP and use it to assess how well it agency has met and delivered its privacy targets.

The agency should start the review process early enough to develop a strong PMP that can be endorsed by management and put into place by the start of the next year (for example, on 1 July). By completing this process in a timely way, the agency will be best placed to highlight priority activities for the coming year to senior management and seek the resources it will need to undertake them.

About this PMP

Agency name	Sport Integrity Australia
PMP commencement date	Wednesday, 29 March 2023
PMP end date	Following commencement, this PMP will operate until Thursday, 28 March 2024.
Recommended review period	Friday, 29 December 2023 to Thursday, 28 March 2024
PMP review date	A review date has not been provided.

Privacy risk profile

In the course of preparing this PMP, the agency has considered various matters relevant to its privacy risk profile. The details of these considerations are provided below for reference.

Privacy risk profile rationale	High risk. The agency handles a broad range of personal information in connection with its functions and activities, including 'sensitive information' and 'health information' of individuals.

Current state

Privacy maturity assessment outcomes

This PMP has been prepared using an assessment of the agency's privacy maturity, the results of which are recorded in the table below. An asterisk (*) next to an attribute name means that it it a 'compliance attribute' and that your agency must have a minimum maturity level of 'Developing' to comply with the Privacy Act or the Code.

Governance & Culture			
Attribute	**Current Level**	**Target Level**	**Rationale/Commentary**

Privacy Champion*	**Developing**	**Defined**	A Privacy Champion has been designated. The General Manager - Corporate (SES1) has responsibility for privacy across the agency. This appointment will be documented in internal policies and procedures, including how the role operates in promoting awareness and reporting to and informing the agency leadership on privacy-related matters.
Privacy Values	**Developing**	**Defined**	There is a connection between the agency's values and respecting and protecting personal information, and staff understand this connection. Staff have general awareness of privacy obligations and secrecy provisions as contained in the SIA Act.
Privacy Officer*	**Developing**	**Defined**	A Privacy Officer has been designated. The Privacy Officer is an EL1 in the Legal Team, and duties may be shared with other staff within the Legal Team when required. The role of the privacy officer will be reflected in agency policies and procedures, including a privacy manual. Contact details to be provided to the OAIC.
Management & Accountability	**Developing**	**Defined**	The agency has assigned responsibility for privacy compliance including senior oversight and operations. The Privacy Champion oversees privacy within the agency, and the Privacy Officer and Legal Team manage privacy issues on a day-to-day basis (e.g. handling complaints and data breaches and providing advice to business areas). Roles and acountabilities for privacy compliance and oversight could be documented and further understood across the agency, and embedded as part of Executive reporting.
Awareness	**Developing**	**Defined**	Staff have a general understanding of privacy obligations and secrecy provisions under the SIA Act. Whole of agency privacy training will occur in 2022, and for new staff upon induction.
Element score (average of attribute scores)			**2 / 4 (Developing)**

Privacy Strategy			
Attribute	**Current Level**	**Target Level**	**Rationale/Commentary**
Privacy Management Plan*	**Developing**	**Defined**	The agency will have a privacy management plan (PMP) in place in 2023. This PMP will be used to track and report on agency compliance and progress against the privacy maturity model to agency leadership bi-annually. For the agency to move from 'Developing' to 'Defined' in the privacy maturity model, the agency should have the PMP endorsed by senior management so that they are made aware of the PMP and the agency's objectives under it.
Inventory of Personal Information*	**Developing**	**Defined**	The agency is developing its inventory of personal information in the form of a register of personal information holdings. A template for reporting on holdings has been developed and disributed to line areas, and responses provided. A completed register will be in place in 2023.
Data Quality Processes*	**Developing**	**Defined**	The agency is starting to define processes to monitor and improve the quality of personal information. Development of privacy resources, and privacy training in 2022 will increase staff awareness of the requirements to ensure that the personal information the agency handles is accurate, up-to-date, complete and relevant. As part of the review of SIA's personal information holdings, the agency will consider whether further guidance in relation to records management is needed.

Information Security Processes	**Developing**	**Defined**	The agency operates within a 'Protected' environment. Staff receive regular training on ICT security including measures such as appropriate use of passes, password security, avoiding spam and phishing emails, and other protective measures. Privacy training in 2022 will increase staff awareness of the requirements of APP11 and of the notifiable data breaches scheme.
Element score (average of attribute scores)			**2 / 4 (Developing)**

Privacy Processes			
Attribute	**Current Level**	**Target Level**	**Rationale/Commentary**
External Privacy Policy & Notices*	**Developing**	**Defined**	The agency privacy policy is available to the public via the agency website. The privacy policy will be reviewed in 2022 to ensure that it is up to date, user friendly, expressed in plain english, transparent and legally compliant. Updated template long form and short form privacy collection notice templates will be made available to all staff in 2023.
Internal Policies & Procedures	**Developing**	**Defined**	There are existing procedures within the agency that have privacy enhancing elements, but few formal internal policies or procedures that are privacy specific. The agency is in the process of reviewing its policies and procedures and will have a privacy manual, privacy fact sheet and other complementary resources in place by the end of 2022. Updated policies and procedures will be communicated to staff to make sure they are understood and followed.
Privacy Training*	**Developing**	**Defined**	Al staff will attend privacy training in 2022. Privacy materials will be completed in 2023 to support the education and training of any new staff or contractors upon induction.

Privacy Impact Assessments*	**Developing**	**Defined**	The agency is aware of its obligations to undertake PIAs where a project is 'high risk'. The agency has a Privacy Impact Assessment Register published on its website. s 47C, s 47E(d) [redacted] The agency will develop its own or utilise the OAIC's Privacy Threshold Assessment template to assist it to identify whether PIAs are necessary. The agency will highlight the requirement for and benefits of undertaking PIAs as part of all staff privacy training in 2022.
Dealing with Suppliers	**Developing**	**Defined**	The agency is reviewing its processes to ensure that all contracts entered into on behalf of the agency incorporate appropriate privacy and confidentiality terms, as required by s 95B of the Privacy Act.
Access & Correction*	**Developing**	**Defined**	The privacy officer is responsible for handling any requests for access or correction, which are infrequent. The agency privacy policy sets out how to request access and correction, and provides a privacy email address for this purpose. The agency has procedures for the management of and response to requests for access and correction. The agency will document these procedures in its Privacy Manual, to be completed by mid-2023.
Complaints & Enquiries	**Developing**	**Defined**	The privacy officer is responsible for handling any privacy complaints, which are infrequent. The agency privacy policy sets out how to make a complaint, and provides a privacy email address for this purpose. The agency has procedures for responding to complaints and enquiries. The agency will document these procedures in its Privacy Manual, to be completed by mid-2023.
Element score (average of attribute scores)			**2 / 4 (Developing)**

Risk & Assurance

Attribute	Current Level	Target Level	Rationale/Commentary
Risk Identification & Assessment	Developing	Defined	The agency identifies privacy risks using available resources and legal support where required. The development of key privacy governance resources and rollout of training in 2022 will enhance the agency's ability to identify, assess and deal with privacy risks.
Reporting & Escalation	Initial	Defined	The agency is responsive to incidents, and escalates and reports to senior leadership on an ad hoc basis. Measures to formalise reporting and escalation of privacy incidents will be considered and developed in 2022 as part of a review of key privacy governance documents (e.g. the finalisation of a Data Breach Response Plan, and considering the role of Privacy Champion in reporting regularly to senior leaderhip on privacy related matters).
Assurance Model	Initial	Defined	First and second line assurance privacy controls are in place through the established functions of the Privacy Officer and Privacy Champion. s 47C, s 47E(d) [redacted]
Element score (average of attribute scores)			1.3 / 4 (Initial)

Data Breach Response			
Attribute	Current Level	Target Level	Rationale/Commentary

Data Breach Response Plan	Initial	Defined	A data breach response plan is being finalised as part of the review of privacy governance documents, and a formal plan will be in place in mid-2023. Efforts have been made to improve awareness of how to identify and respond to data breaches.
Data Breach Notification*	Developing	Defined	Data breaches can be reported to the Privacy Officer. The Privacy Officer is responsible for notifying the OAIC and individuals. Data breach identification, assessment, mitigation and notification will be addressed in whole of agency privacy training in 2022.
Element score (average of attribute scores)			1.5 / 4 (Initial)

Average of element scores	1.8 / 4
Overall privacy maturity level	2 / 4 (Developing)

Adequacy of privacy policy and notices

Section 17 of the Code requires an agency to regularly assess the adequacy of its privacy practices, procedures and systems (including its privacy policy and collection notices) to ensure their adequacy for the purpose of compliance with the APPs and currency. Generally, completion of a PMP facilitates compliance with this requirement.

The outcomes of the agency's review of its privacy policy and collection notices are recorded below.

Privacy Policy (APP 1) Compliance Gaps	Privacy Policy is in place, and will be be reviewed in 2023 to check compliance.
Privacy Policy (APP 1) Currency Gaps	Updated Privacy Policy to be reviewed and finalised to ensure it reflects all of the agency's functions and activities
Privacy Notices (APP 5) Compliance Gaps	General template notices to be developed in 2023. Athletes Privacy Statement is in place.
Privacy Notices (APP 5) Currency Gaps	General template developed awaiting endorsement. Athletes Privacy Statement is in place.

Goals for improvement

The privacy goals and targets in this section are based on the agency's privacy maturity assessment outcomes. This section includes mandatory actions which the agency must take in order to meet its compliance obligations under APP 1.2 (Code, s 9(2)(b)).

Compliance Actions

Where the agency has identified in its privacy maturity assessment that it is at the 'Initial' level in relation to a compliance attribute, this indicates that there is a compliance gap because the agency must have a minimum maturity level of 'Developing' for that attribute in order to comply with the Privacy Act or the Code. All compliance gaps must form part of this PMP and may require prompt remediation. Remediation actions are set out below.

Attribute	Remediation action	Responsible person, position or team	Due	Required resources, dependencies and/or related documents (specify or link)
There are no compliance actions defined in this PMP.				

Privacy Policy & Notices Actions

Remediation actions related to any gaps in the adequacy of the agency's Privacy Policy (APP 1) or Privacy Notices (APP 5) are captured below.

Attribute	Remediation actions	Responsible person, position or team	Due	Required resources, dependencies and/or related documents (specify or link)

Privacy Policy (APP 1)	Reviewing privacy policy to ensure it is up-to-date, and reflects the functions and activities of the agency, and the types of collections that may occur.	Privacy Officer, Legal Team	1/05/2023	
Privacy Notices (APP 5)	Athletes Statement is in place. Agency is preparing template privacy notices to be utilised by business areas when collecting personal information.	Privacy Officer, Legal Team	1/05/2023	

Maturity Improvement Actions

The table below sets out actions which the agency plants to achieve in order to improve its privacy maturity. Any uncompleted actions from previous PMPs which are still relevant should also be documented in this section to ensure that they form part of the agency's next PMP.

Element / Attribute	Action	Responsible person, position or team	Due	Required resources, dependencies and/or related documents (specify or link)

Governance & Culture / Privacy Champion	Privacy Officer to work with Privacy Champion to promote a culture of privacy that values and protects personal information, and supports the integration of privacy practices, procedures and systems into broader organisational frameworks. Privacy awareness raising activities to occur in privacy awareness week and throughout the year. s 47C, s 47E(d) Privacy Champion to report regularly to senior leadership.	Privacy Officer Privacy Champion	31/10/2023	
Governance & Culture / Privacy Values	Privacy governance documents to be developed and distributed to staff (possibly via a dedicated intranet page). Privacy training in 2022 will emphasise the importance of privacy as a core value that is central to the reputation of the agency.	Privacy Officer & ICT	1/05/2023	

Governance & Culture / Privacy Officer	The designated Privacy Officer will establish practices, procedures and systems to support their obligations. These will be documented as part of a privacy governance review by mid-2023. Reporting frameworks will be considered to embed broader privacy awareness for senior leadership and across the agency. Further Privacy training will occur in 2023 will build awareness of the role of the Privacy Officer and enable broader privacy compliance.	Privacy Officer Privacy Champion	31/10/2023	
Governance & Culture / Management & Accountability	Privacy Management Plan and key privacy policies and procedural documents to be approved by senior leadership, and regular review and approval to be scheduled. Execeutive reporting will be considered to ensure visibility of high risk privacy issues, and to assist the agency to track activity against this PMP.	Privacy Officer Privacy Champion	1/05/2023	

Governance & Culture / Awareness	Changes to policies and procedures will be distributed to staff. Privacy training will be provided to all staff in 2023.	Privacy Officer	1/05/2023	
Privacy Strategy / Privacy Management Plan	PMP will be endorsed by Executive in 2023, and implemented by the Privacy Officer and Privacy Champion. Privacy Officer and Privacy Champion will consider options for s 47C, s 47E(d) [redacted]	Privacy Officer Privacy Champion Executive	1/05/2023	
Privacy Strategy / Inventory of Personal Information	Register of Personal Information Holdings will be endorsed by Executive, and procedures developed for it to be reviewed on an annual basis. Template emails to inform the register will be provided to business areas when there is a change of structure, or at each review point.	Privacy Officer Executive	1/05/2023	

Privacy Strategy / Data Quality Processes	Privacy documents, including the privacy manual and privacy fact sheet, will be disributed to staff to inform them of the need to maintain quality of personal information. All staff training in 2022 will embed understanding by agency personnel of obligations with respect to the quality of personal information.	Privacy Officer	1/05/2023	

Privacy Strategy / Information Security Processes	The agency has existing policies in respect of securing its premises and information holdings, and staff are aware of this. Procedural documents, such as the privacy manual and factsheet, set out relevant information, and provide links to other resources to assist staff in securing personal information. A data breach response plan will be endorsed in 2023, and will assist staff to understand their obligations in relation to preventing and mitigating data breaches. Further consideration will be given to other measures that may be taken to boost protection of personal information. ICT will update and publish its Information Security Policies on SharePoint.	Privacy Officer ICT	1/05/2023	
Privacy Processes / External Privacy Policy & Notices	Privacy Policy is being reviewed and will be endorsed in 2023. Privacy notice templates are being developed and will be endorsed in 2023.	Privacy Officer Privacy Champion	1/05/2023	

Privacy Processes / Internal Policies & Procedures	A comprehensive privacy governance review is underway, and policies and procedures will be in place in 2023.	Privacy Officer	1/05/2023	
Privacy Processes / Privacy Training	Privacy training materials are being developed and finalised in 2022. All agency privacy training will take place in 2022, and then on an annual basis, and for new personnel upon induction.	Privacy Officer	Complete	
Privacy Processes / Privacy Impact Assessments	The privacy manual and fact sheet (to be endorsed in 2023) will set out requirements for the conduct of PIAs. Consideration will be given to any additional resources/templates that may be required. OAIC resources will be leveraged and referred to in the privacy manual. All agency privacy training in 2022 will emphasise the requirement for PIAs for all high risk privacy projects involving new or changed ways of handling personal information.	Privacy Officer	1/05/2023	

Privacy Processes / Dealing with Suppliers	Privacy Officer to review agency processes for assessing third party contracts to ensure privacy requirements are met.	Privacy Officer	1/05/2023	
Privacy Processes / Access & Correction	Privacy manual will be put in place by mid 2023 that addresses process for action and correction. Privacy training for all staff in 2022 will address access and correction.	Privacy Officer	1/05/2023	
Privacy Processes / Complaints & Enquiries	Privacy manual will incorporate processes for dealing with privacy enquiries and complaints. All agency privacy training in 2022 will empower staff to respond appropriately to enquiries and complaints.	Privacy Officer	1/05/2023	

Risk & Assurance / Risk Identification & Assessment	Privacy governance review will ensure strong, clear and consistent processes that will aid agency staff to identify and assess privacy risks. Privacy Officer and Privacy Champion will manage risks, and make these visible to Executive through regular reporting.	Privacy Officer	As required	
Risk & Assurance / Reporting & Escalation	Privacy Officer and Privacy Champion to consider options for executive reporting and incident escalation. Privacy Officer and Privacy Champion to consider integrating privacy into broader risk management and planning processes.	Privacy Officer	31/10/2023	

Risk & Assurance / Assurance Model	Privacy Officer and Privacy Champion to consider options for executive reporting and incident escalation. Privacy Officer and Privacy Champion to consider integrating privacy into broader risk management and planning processes.	Privacy Officer	31/10/2023	
Data Breach Response / Data Breach Response Plan	Comprehensive data breach response plan will be endorsed by mid-2023. All agency training in 2022 will educate staff on how to identify, contain and escalate data breaches. Agency to develop process for reporting data breaches to Executive.	Privacy Officer	31/10/2023	

Data Breach Response / Data Breach Notification	Data breach response plan addresses notification requirements. Privacy Officer will have responsibility for notifying breaches externally, and will seek legal advice where necessary.	Privacy Officer	N/A	
Governance & Culture / Privacy Champion	s 47C, s 47E(d)	Privacy Champion & Executive		

Bringing the PMP together and prioritising actions

This section of the PMP identified all compliance actions and actions for improvement, as well as who is responsible for delivery of each action, interdependencies and due dates. From here, prioritisation is a key part of establishing an achievable PMP. Agencies should take a risk-based approach to prioritising and timing their improvement activities.

Measure performance

It is expected that the agency will review this PMP during the time in which it is active in order to document progress against the actions described above.

The table below provides a central location to track progress.

Action	Achieved	Future actions / commentary
Reviewing privacy policy to ensure it is up-to-date, and reflects the functions and activities of the agency, and the types of collections that may occur.		

Athletes Statement is in place. Agency is preparing template privacy notices to be utilised by business areas when collecting personal information.		
Privacy Officer to work with Privacy Champion to promote a culture of privacy that values and protects personal information, and supports the integration of privacy practices, procedures and systems into broader organisational frameworks. Privacy awareness raising activities to occur in privacy awareness week and throughout the year. s 47C, s 47E(d) Privacy Champion to report regularly to senior leadership.		
Privacy governance documents to be developed and distributed to staff (possibly via a dedicated intranet page). Privacy training in 2022 will emphasise the importance of privacy as a core value that is central to the reputation of the agency.		

The designated Privacy Officer will establish practices, procedures and systems to support their obligations. These will be documented as part of a privacy governance review by mid-2023. Reporting frameworks will be considered to embed broader privacy awareness for senior leadership and across the agency. Further Privacy training will occur in 2023 will build awareness of the role of the Privacy Officer and enable broader privacy compliance.		
Privacy Management Plan and key privacy policies and procedural documents to be approved by senior leadership, and regular review and approval to be scheduled. Execeutive reporting will be considered to ensure visibility of high risk privacy issues, and to assist the agency to track activity against this PMP.		
Changes to policies and procedures will be distributed to staff. Privacy training will be provided to all staff in 2023.		
PMP will be endorsed by Executive in 2023, and implemented by the Privacy Officer and Privacy Champion. Privacy Officer and Privacy Champio s 47C, s 47E(d) [redacted]		

Register of Personal Information Holdings will be endorsed by Executive, and procedures developed for it to be reviewed on an annual basis. Template emails to inform the register will be provided to business areas when there is a change of structure, or at each review point.		
Privacy documents, including the privacy manual and privacy fact sheet, will be disributed to staff to inform them of the need to maintain quality of personal information. All staff training in 2022 will embed understanding by agency personnel of obligations with respect to the quality of personal information.		
The agency has existing policies in respect of securing its premises and information holdings, and staff are aware of this. Procedural documents, such as the privacy manual and factsheet, set out relevant information, and provide links to other resources to assist staff in securing personal information. A data breach response plan will be endorsed in 2023, and will assist staff to understand their obligations in relation to preventing and mitigating data breaches. Further consideration will be given to other measures that may be taken to boost protection of personal information. ICT will update and publish its Information Security Policies on SharePoint.		

Privacy Policy is being reviewed and will be endorsed in 2023. Privacy notice templates are being developed and will be endorsed in 2023.		
A comprehensive privacy governance review is underway, and policies and procedures will be in place in 2023.		
Privacy training materials are being developed and finalised in 2022. All agency privacy training will take place in 2022, and then on an annual basis, and for new personnel upon induction.		
The privacy manual and fact sheet (to be endorsed in 2023) will set out requirements for the conduct of PIAs. Consideration will be given to any additional resources/templates that may be required. OAIC resources will be leveraged and referred to in the privacy manual. All agency privacy training in 2022 will emphasise the requirement for PIAs for all high risk privacy projects involving new or changed ways of handling personal information.		

Privacy Officer to review agency processes for assessing third party contracts to ensure privacy requirements are met.		
Privacy manual will be put in place by mid-2023 that addresses process for action and correction. Privacy training for all staff in 2022 will address access and correction.		
Privacy manual will incorporate processes for dealing with privacy enquiries and complaints. All agency privacy training in 2022 will empower staff to respond appropriately to enquiries and complaints.		
Privacy governance review will ensure strong, clear and consistent processes that will aid agency staff to identify and assess privacy risks. Privacy Officer and Privacy Champion will manage risks, and make these visible to Executive through regular reporting.		

Privacy Officer and Privacy Champion to consider options for executive reporting and incident escalation. Privacy Officer and Privacy Champion to consider integrating privacy into broader risk management and planning processes.		
Privacy Officer and Privacy Champion to consider options for executive reporting and incident escalation. Privacy Officer and Privacy Champion to consider integrating privacy into broader risk management and planning processes.		
Comprehensive data breach response plan will be endorsed by mid-2023. All agency training in 2022 will educate staff on how to identify, contain and escalate data breaches. Agency to develop process for reporting data breaches to Executive.		

Data breach response plan addresses notification requirements. Privacy Officer will have responsibility for notifying breaches externally, and will seek legal advice where necessary.		
s 47C, s 47E(d)		

Privacy Management Plan

Sport Integrity Australia

31 March 2025 to 31 March 2026

Background

What is a Privacy Management Plan?

A Privacy Management Plan (**PMP**) is a document that identifies specific, measurable privacy goals and targets and sets out how an agency will meet its compliance obligations under APP 1.2. An agency must measure and document its performance against its Privacy Management Plan at least annually.

Before developing a PMP, every agency will need to understand the current state of their privacy practices. Agencies should refer to the OAIC's *Interactive PMP Explained* resource for guidance on how to identify compliance gaps and opportunities to improve maturity.

What are the next steps?

This PMP describes the actions that the agency must take in order to meet its privacy compliance obligations and maturity targets for the year following the PMP's commencement date (specified below). The agency must take steps to achieve these actions and to record how it has done so.

This PMP should be kept up to date over the course of the year. In the recommended review period (specified below), the agency should return to this PMP and use it to assess how well the agency has met and delivered its privacy targets.

The agency should start the review process early enough to develop a strong PMP that can be endorsed by management and put into place by the start of the next year (for example, on 1 July). By completing this process in a timely way, the agency will be best placed to highlight priority activities for the coming year to senior management and seek the resources it will need to undertake them.

About this PMP

Agency name	Sport Integrity Australia
PMP commencement date	Monday, 31 March 2025

PMP end date	Following commencement, this PMP will operate until Tuesday, 31 March 2026
Recommended review period	Wednesday, 31 December 2025 to Tuesday, 31 March 2026
PMP review date	A review date has not been provided

Privacy risk profile

In the course of preparing this PMP, the agency has considered various matters relevant to its privacy risk profile. The details of these considerations are provided below for reference.

Privacy risk profile rationale	High risk. The agency handles a broad range of personal information in connection with its functions and activities, including 'sensitive information' and 'health information' of individuals.

Current state

Privacy maturity assessment outcomes

This PMP has been prepared using an assessment of the agency's privacy maturity, the results of which are recorded in the table below. An asterisk (*) next to an attribute name means that it is a 'compliance attribute' and that your agency must have a minimum maturity level of 'Developing' to comply with the Privacy Act or the Code.

Governance & Culture			
Attribute	**Current Level**	**Target Level**	**Rationale/Commentary**
Privacy Champion*	**Defined**	**Defined**	A Privacy Champion has been designated to the position of Deputy CEO – Strategy, International Policy & Corporate (SES2). The role of the agency's Privacy Champion is documented in internal policies and procedures, including how the role operates in promoting awareness and reporting to, and informing, the agency's leadership on privacy-related matters.
Privacy Values	**Developing**	**Defined**	s 47C, s 47E(d)

Privacy Officer*	Defined	Defined	The Privacy Officer role is delegated to members of the Legal Team, and is reflected in the agency's policies and procedures, including the Privacy Manual Procedure.
Management & Accountability	Defined	Defined	The agency has assigned responsibility for privacy compliance including senior oversight and operations. The Privacy Champion oversees privacy within the agency, and the Privacy Officer/Legal Team manage privacy issues on a day-to-day basis (e.g. handling complaints and data breaches and providing advice to business areas).
Awareness	Developing	Defined	Staff have a general understanding of privacy obligations and secrecy provisions under the SIA Act. Whole-of-agency privacy training will be conducted and is mandatory for new staff on induction.
Element score (average of attribute scores)			2 / 5 (Developing)

Privacy Strategy			
Attribute	Current Level	Target Level	Rationale/Commentary
Privacy Management Plan*	Defined	Defined	The agency has a PMP in place.
Inventory of Personal Information*	Defined	Defined	The agency has a register of personal information holdings which is distributed to business areas annually for updating.
Data Quality Processes*	Developing	Defined	The agency is continuing to define processes to monitor and improve the quality of personal information. Development of privacy resources and privacy training has increased staff awareness of the requirements to ensure that the personal information the agency collects and handles is accurate, up-to-date, complete and relevant.
Information Security Processes	Defined	Defined	The agency operates within a 'Protected' environment. Staff receive regular training on ICT security including measures such as appropriate use of passes, password security, avoiding spam and phishing emails, and other protective measures. Privacy training has increased staff awareness of the requirements of the APPs and the Notifiable Data Breaches scheme.
Element score (average of attribute scores)			1 / 4 (Developing)

Privacy Processes			
Attribute	**Current Level**	**Target Level**	**Rationale/Commentary**
External Privacy Policy & Notices*	**Defined**	**Defined**	The Privacy Policy is available on the agency's website, and is reviewed regularly to ensure that it is up to date, user friendly, expressed in plain English, transparent and legally compliant.
Internal Policies & Procedures	**Defined**	**Defined**	The agency has a Privacy Policy, Privacy Manual Procedure, PMP, Privacy Collection Notice Templates, Data Breach Response Plan Policy, and ASDMAC Privacy Policy in place.
Privacy Training*	**Developing**	**Defined**	All staff will attend privacy training when held, and upon induction.
Privacy Impact Assessments*	**Developing**	**Defined**	The agency is aware of its obligation to undertake PIAs where a project is 'high risk'. Information about the requirement for, and benefits of, undertaking PIAs is included in the agency's Privacy Policy. The Legal team also advises staff to complete PIAs where applicable (e.g. when reviewing a contract for a new 'high risk' project for a business area).
Dealing with Suppliers	**Defined**	**Defined**	The agency is reviewing its processes to ensure that all contracts entered into on behalf of the agency incorporate appropriate privacy and confidentiality terms, as required by s 95B of the Privacy Act.
Access & Correction*	**Defined**	**Defined**	The Privacy Officer/Legal team is responsible for handling any requests for access or correction, which are infrequent. The Privacy Policy sets out how to request access to and correction/amendment of personal information and provides a privacy email address for this purpose. The agency has procedures for the management of and response to requests for access and correction/amendment set out in the Privacy Manual Procedure.
Complaints & Enquiries	**Defined**	**Defined**	The Privacy Officer/Legal team is responsible for handling any privacy complaints, which are infrequent. The Privacy Policy sets out how to make a complaint and provides a privacy email address for this purpose. The agency has procedures for responding to complaints and enquiries set out in the Privacy Manual Procedure.
Element score (average of attribute scores)			**2 / 7 (Developing)**

Risk & Assurance			
Attribute	**Current Level**	**Target Level**	**Rationale/Commentary**
Risk Identification & Assessment	**Developing**	**Defined**	The agency identifies privacy risks using available resources and legal support where required.
Reporting & Escalation	**Defined**	**Defined**	The agency is responsive to incidents, and escalates and reports to senior leadership in line with the Data Breach Response Plan and other applicable policies/procedures.
Assurance Model	**Developing**	**Defined**	First and second line assurance privacy controls are in place through the established functions of the Privacy Officer and Privacy Champion. s 47C, s 47E(d) [redacted]
Element score (average of attribute scores)			**2/ 3 (Developing)**

Data Breach Response			
Attribute	**Current Level**	**Target Level**	**Rationale/Commentary**
Data Breach Response Plan	**Defined**	**Defined**	A Data Breach Response Plan is in place.
Data Breach Notification*	**Defined**	**Defined**	Data breaches are reported to the Privacy Officer and Privacy Champion. The Privacy Officer/Privacy Champion are responsible for notifying the OAIC and individuals where a breach is considered a 'Notifiable Data Breach' under the Privacy Act and Notifiable Data Breach scheme.
Element score (average of attribute scores)			**2 / 2 (Defined)**

Overall privacy maturity level	**7 / 21 (Developing)**

Adequacy of privacy policy and notices

Section 17 of the Code requires an agency to regularly assess the adequacy of its privacy practices, procedures and systems (including its privacy policy and collection notices) to ensure their adequacy for the purpose of compliance with the APPs and currency. Generally, completion of a PMP facilitates compliance with this requirement.

The outcomes of the agency's review of its privacy policy and collection notices are recorded below.

Privacy Policy (APP 1) Compliance Gaps	Privacy Policy is in place and is reviewed annually to ensure compliance.
Privacy Policy (APP 1) Currency Gaps	Privacy Policy is in place and is reviewed annually to ensure compliance.
Privacy Notices (APP 5) Compliance Gaps	General template notices and Athletes Privacy Statement in place.
Privacy Notices (APP 5) Currency Gaps	General template notices and Athletes Privacy Statement in place.

Goals for improvement

The privacy goals and targets in this section are based on the agency's privacy maturity assessment outcomes. This section includes mandatory actions which the agency must take in order to meet its compliance obligations under APP 1.2 (Code, s 9(2)(b)).

Compliance Actions

Where the agency has identified in its privacy maturity assessment that it is at the 'Initial' level in relation to a compliance attribute, this indicates that there is a compliance gap because the agency must have a minimum maturity level of 'Developing' for that attribute in order to comply with the Privacy Act or the Code. All compliance gaps must form part of this PMP and may require prompt remediation. Remediation actions are set out below.

Attribute	Remediation action	Responsible person, position or team	Due	Required resources, dependencies and/or related documents (specify or link)
There are no relevant compliance actions defined in this PMP.				

Privacy Policy & Notices Actions

Remediation actions related to any gaps in the adequacy of the agency's Privacy Policy (APP 1) or Privacy Notices (APP 5) are captured below.

Attribute	Remediation actions	Responsible person, position or team	Due	Required resources, dependencies and/or related documents (specify or link)
There are no remediation actions required in relation to the adequacy of the agency's Privacy Policy (APP 1) or Privacy Notices (APP 5).				

Maturity Improvement Actions

The table below sets out actions which the agency plans to achieve in order to improve its privacy maturity. Any uncompleted actions from previous PMPs which are still relevant should also be documented in this section to ensure that they form part of the agency's next PMP.

Element / Attribute	Action	Responsible person, position or team	Due	Required resources, dependencies and/or related documents (specify or link)
Governance & Culture / Privacy Champion	Privacy Officer to continue to work with the Privacy Champion to promote a culture of privacy that values and protects personal information, and supports the integration of privacy practices, procedures and systems into broader organisational frameworks. Privacy awareness raising activities to occur in the OAIC's Privacy Awareness Week and throughout the year.	Privacy Officer and Privacy Champion	Ongoing	

Bringing the PMP together and prioritising actions

This section of the PMP identified all compliance actions and actions for improvement, as well as who is responsible for delivery of each action, interdependencies and due dates. From here, prioritisation is a key part of establishing an achievable PMP. Agencies should take a risk-based approach to prioritising and timing their improvement activities.

Measure performance

It is expected that the agency will review this PMP during the time in which it is active in order to document progress against the actions described above.

The table below provides a central location to track progress.

Action	Achieved	Future actions / commentary
Reviewing Privacy Policy to ensure it is up-to-date, and reflects the functions and activities of the agency, and the types of collections that may occur.	Ongoing	Annual review of privacy policies/procedures.
Privacy Officer to work with Privacy Champion to promote a culture of privacy that values and protects personal information, and supports the integration of privacy practices, procedures and systems into broader organisational frameworks. Privacy awareness raising activities to occur in the OAIC's Privacy Awareness Week and throughout the year.	Ongoing	Ongoing

Privacy training – Sport Integrity Australia

s 47F

Australian Government Solicitor

s 22

s 22

s 22

s 22

s 22

s 22

s 22

s 22

s 22


S 22

s 22

s 22

s 22

s 22

s 22

s 22

s 22


s 22

Privacy (Australian Government Agencies – Governance) Code 2017

s 22

- Privacy Impact Assessments

s 22

Privacy Impact Assessments & Project Planning

- PIAs are required for any project that involves new or changed personal information handling that are high risk.

- **Examples**
  - Handling large amounts of personal information
  - Handling sensitive information
  - Handling existing information for new or multiple purposes
  - Information about vulnerable people/sensitive information

When entering into third party contracts/arrangements

SIA must take contractual measures to ensure APP privacy compliance by its contractors/third-party agents (s 95B). Contracts should also address:

- what will happen in the event of a data breach
- preventing access or storage of personal information outside Australia
- requiring security clearances and/or undertakings to keep personal information confidential and secure
- limit access to only the information that is required to provide the contract services for the contract purposes
- ISPPPI mandates that you assess to ensure that they can provide sufficient guarantees for the safeguarding of personal information

s 22


S 22


s 22

s 22

s 22


s 22

In summary - When should I consider privacy?

- During project planning
- Before and when collecting personal information
- Before using or disclosing personal information
- Before disclosing personal information to overseas recipients
- Before accessing personal information
- When considering the quality of information
- When entering a Commonwealth contract, or working with third-party agents
- When receiving requests for access to personal information

Questions?

Thank you

Australian Government
Sport Integrity Australia

SPORT INTEGRITY AUSTRALIA

Procedure

Privacy Manual

Procedure owner: Legal

Endorsed by: Luke McCann, Deputy Chief Executive Officer – Strategy, International Policy & Corporate and Privacy Champion

Date endorsed: 3 April 2025

Next review date: October 2026

Contents


S 22

s 22

s 22

s 22

s 22

s 22

s 22

s 22

s 22

3. Privacy Impact Assessments

The Privacy Code requires us to undertake a Privacy Impact Assessment (**PIA**) for all 'high privacy risk' projects or initiatives that involve new or changed ways of handling personal information. A project will be 'high risk' if it is likely to have a significant impact on the privacy of individuals.

When developing a project that involves new or changed personal information handling practices, you must advise your managers and conduct a Privacy Threshold Assessment (**PTA**) to determine whether a PIA should be conducted. You should also engage the Privacy Officer during the planning phase.

Undertaking a PIA is one way in which we can ensure it has regard to privacy risks of a new project or initiative in the development and implementation stages. This means that we not only maintain best practice in collecting and handling personal information, but also, we reduce the likelihood of any data or privacy breaches by considering ways of managing, minimising or eliminating any impacts on privacy.

In accordance with the Privacy Code, we maintain a register of the PIAs we conduct and publish the register on our website.

Resources

Part 3 Privacy Code

Guide to undertaking privacy impact assessments (OAIC)

When do agencies need to conduct a privacy impact assessment? (OAIC)

s 22

s 22

s 22

s 22

s 22

s 22

s 22

s 22

s 22

s 22


S 22

s 22


s 22

s 22

s 22

Australian Government
Sport Integrity Australia

SPORT INTEGRITY AUSTRALIA

Privacy – Getting it right

Policy owner: Legal

Endorsed by: Bill Turner, Privacy Champion, and General Manager – Corporate

Date endorsed: 17 April 2023

Next review date: October 2024


s 22

s 22

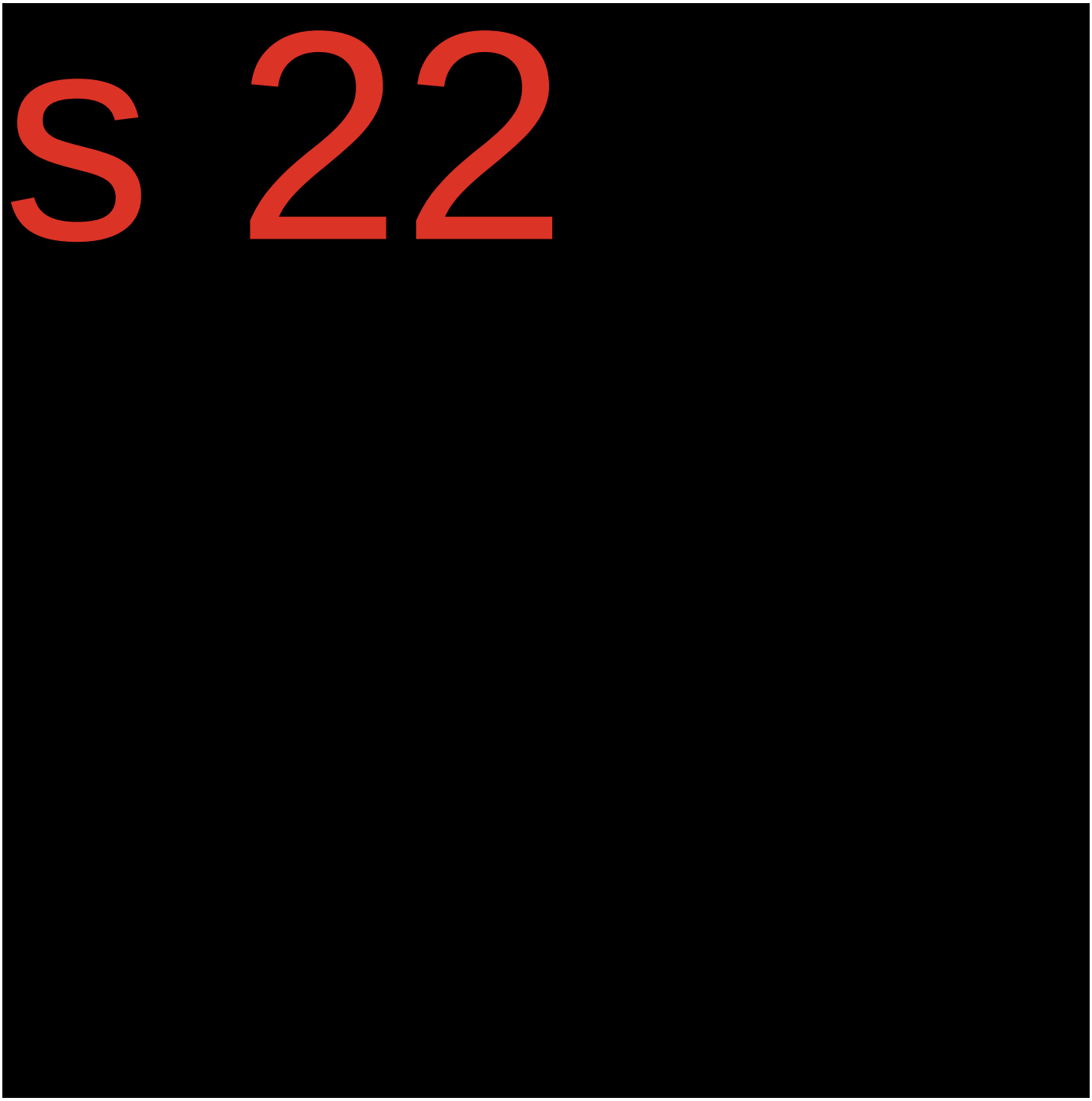
When should I consider privacy?

During project planning or entering contracts

When developing a project that involves new or changed personal information handling practices, you must always consider whether a Privacy Impact Assessment (PIA) is required.

You must advise your managers or leadership team of any projects or proposals involving new or changed ways of handling personal information and engage a Privacy Officer during the planning phase.

You ***must*** undertake a PIA for all 'high risk' projects. Generally, a high-risk project is anything that involves a new or changed way of handling personal information. However, there is no hard-and-fast rule about whether a PIA will be necessary. You can do a PIA for any project, whether it is high or low risk. A PIA identifies how a project may impact on individuals' privacy and makes recommendations for managing, minimising or eliminating privacy impacts. Completing a Privacy Threshold Assessment (PTA) can also assist to assess whether a PIA is necessary.



s 22

s 22

11

s 22

Privacy Awareness Week - what you might have missed

s 22, s 47F

Day 2

What is a PIA?

A PIA is a systemic assessment of a project that identifies potential privacy impacts and recommendations to manage, minimise or eliminate them. A PIA reflects a 'privacy by design' approach, which embeds good privacy practices into the design of a new project or system, rather than tacking it on at the end. It's about managing privacy risks proactively, rather than retrospectively.

A 'project' means activities and initiatives that may have privacy implications, like policy proposals, new systems or databases, new methods or procedures for service delivery or information handling or changes to how information is stored.

A PIA is conducted by comparing your project to the 13 Australian Privacy Principles (APPs). During a PIA, each APP is examined to see whether it's applicable to your

project, and any impacts the project may have on those APPs. A guide of the APPs is **attached** for your information.

All government agencies are obliged to undertake a PIA for all high privacy risk projects in accordance with the Privacy (Australian Government Agencies – Governance) APP Code 2017 (the Code).

How do we determine what is a 'high privacy risk'?

In order to determine whether a project is a 'high privacy risk', we are required to conduct a Privacy Threshold Assessment (PTA). This assessment is completed by the business area and the Privacy team (our friendly Legal Team) are available to assist if required. If you consider that an upcoming project may require a PTA or a PIA, please email privacy@sportintegrity.gov.au.

If you want to learn more about PIA's, the below links from the Office of the Australian Information Commissioner provide useful guides:

- PIA resources
- For Australian Government agencies: When is a PIA needed?

More information about PIA's is contained in our brand-new Privacy Manual available on the Policies Page on SharePoint. This is a useful tool for all staff to consider when they have questions about privacy. It sets out our key practices,

s 22

s 22

s 22

s 22

- You should contact the privacy team for assistance in conducting a Privacy Threshold Assessment (PTA) or a Privacy Impact Assessment (PIA) if you are developing or reviewing a project that handles personal information.

s 22


S 22

Outlook

[Draft] Fw: Privacy Awareness Week - Day 1 - Privacy Impact Assessments

s 47F [redacted]

Draft saved Thu 14-May-2026 2:51 PM

3 attachments (9 MB)
APP Quick Reference.pdf; image001.jpg; image002.jpg;

From: SIA - Privacy
Sent: Monday, June 05, 2023 1:45 PM
To: SIA All Staff (excluding DCOs)
Subject: Fw: Privacy Awareness Week - Day 1 - Privacy Impact Assessments

OFFICIAL

Dear colleagues,

Welcome to day 2 of Privacy Awareness Week!

Today we are discussing privacy impact assessments. Are you developing or reviewing a project? Consider the need for a privacy impact assessment (PIA). You should conduct a PIA as part of your risk management and planning processes.

What is a PIA?

A PIA is a systemic assessment of a project that identifies potential privacy impacts and recommendations to manage, minimise or eliminate them. A PIA reflects a 'privacy by design ' approach, which embeds good privacy practices into the design of a new project or system, rather than tacking it on at the end. It 's about managing privacy risks proactively, rather than retrospectively.

A 'project ' means activities and initiatives that may have privacy implications, like policy proposals, new systems or databases, new methods or procedures for service delivery or information handling or changes to how information is stored.

A PIA is conducted by comparing your project to the 13 Australian Privacy Principles (APPs). During a PIA, each APP is examined to see whether it 's applicable to your project, and any impacts the project may have on those APPs. A guide of the APPs is **attached** for your information.

All government agencies are obliged to undertake a PIA for all high privacy risk projects in accordance with the Privacy (Australian Government Agencies – Governance) APP Code 2017 (the Code).

How do we determine what is a 'high privacy risk '?

In order to determine whether a project is a 'high privacy risk ', we are required to conduct a Privacy Threshold Assessment (PTA). This assessment is completed by the business area and the Privacy team (our friendly Legal Team) are available to assist if required. If you consider that an upcoming project may require a PTA or a PIA, please email privacy@sportintegrity.gov.au.

If you want to learn more about PIA 's, the below links from the Office of the Australian Information Commissioner provide useful guides:

- PIA resources
- For Australian Government agencies: When is a PIA needed?

More information about PIA 's is contained in our brand-new Privacy Manual available on the Policies Pageon SharePoint. This is a useful tool for all staff to consider when they have questions about privacy. It sets out our key practices, procedures and processes for handling personal information to ensure we comply with the relevant privacy laws when we carry out our functions and duties at SIA.

Quiz

Don 't forget to challenge yourself with the OAIC 's quick quiz. Once you have completed the quiz, be sure to download the certificate of completion and send to privacy@sportintegrity.gov.au for your chance to win a $100 debit gift card. Entries close at 5:00pm on Friday, 5 May 2023.

Kind regards,

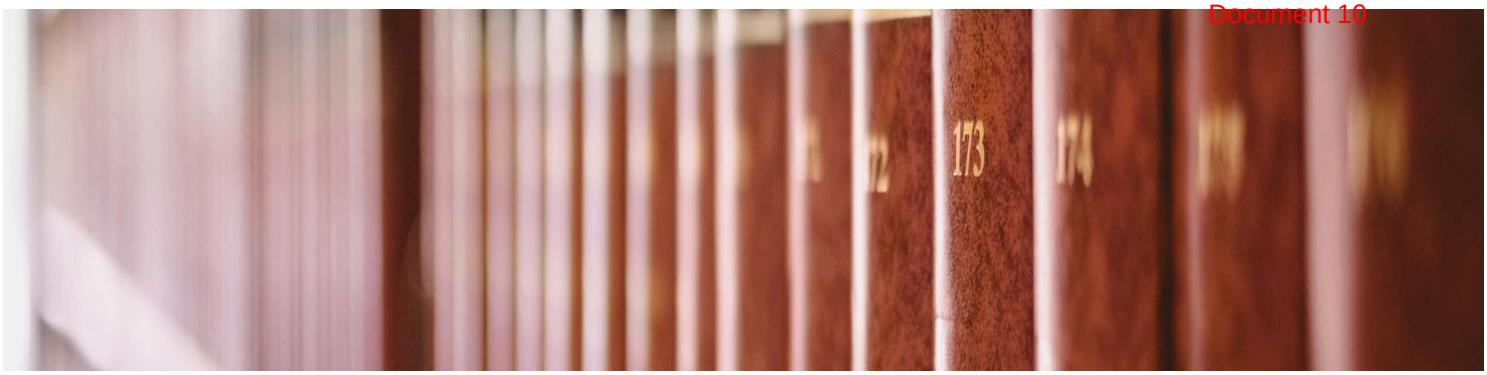
SPORT INTEGRITY AUSTRALIA

Privacy Team - Sport Integrity Australia

e | privacy@sportintegrity.gov.au

PROTECTING SPORT TOGETHER | **sportintegrity.gov.au** |

OFFICIAL



David Pammenter
Legal Advisor

2 min read

s 22

Before starting a project or changing a business process, consider conducting a Privacy Impact Assessment with help from the Legal team, to identify and address potential privacy risks.

s 22


s 22

SPORT INTEGRITY AUSTRALIA

PRIVACY TRAINING

May 2024

S 22

s 22

s 22

S 22

[redacted]

S 22

s 22

s 22

s 22


S 22


s 22


S 22


S 22


S 22


s 22

s 22


s 22

s 22

[redacted]


S 22

Privacy (Australian Government Agencies – Governance) Code 2017

s 22

- Privacy Impact Assessments

s 22

s 22


s 22


s 22

s 22


s 22


s 22


S 22


S 22


s 22

Privacy Impact Assessments

The Office of the Australian Information Commissioner recommends conducting a Privacy Impact Assessment when you start a new project or change a business process. In some cases, it is a requirement under the Privacy Code to conduct a Privacy Impact Assessment, e.g. when a project contains sensitive information or is considered high risk.

A Privacy Impact Assessment helps you to identify the impact the project or change might have on the privacy of individuals and sets out recommendations for managing, minimising, or eliminating that impact.

Before completing a Privacy Impact Assessment, we recommend you complete a Privacy Threshold Assessment to determine if a Privacy Impact Assessment is required.


S 22


S 22

s 22

s 22

Outlook

[Draft] Fw: Privacy Impact Assessment for s 47E(d)

s 47F
Draft saved Tue 12-May-2026 9:04 AM

9 attachments (187 KB)
Threshold assessment template.docx; image001.jpg; image002.jpg; image004.jpg; image006.jpg; image008.jpg; image009.jpg; image010.jpg; image011.jpg;

s 47F
Sent: Friday, October 13, 2023 1:18 PM
s 47F
Cc: SIA - Privacy; s 47F
Subject: Fw: Privacy Impact Assessment for s 47E(d)

OFFICIAL: Sensitive

Hi Investigations,

As discussed this morning, please see attached threshold assessment template for completion in relation to the agency 's use s 47E(d)

The threshold assessment template is designed to assist agencies in identifying when a privacy impact assessment (PIA) should be completed, however, in this case, we recommend a PIA is completed, which legal can assist with. If you can complete the threshold assessment template, that will help us collect the information we need for the assessment.

Just for your background, the Privacy (Australian Government Agencies – Governance) APP Code 2017 (**the Code**) requires Australian Government agencies subject to the Privacy Act to conduct a privacy impact assessment (**PIA**) for all 'high privacy risk projects '. A project may be a high privacy risk project if the agency reasonably considers that the project involves new or changed ways of handling personal information that are likely to have a significant impact on the privacy of individuals.

A PIA is a systematic assessment of a project that identifies the impact the project may have on the privacy of individuals, and sets out recommendations for managing, minimising, or eliminating that impact.

If you can also explain how the software works, what 's involved in its use, or provide any background procedures that investigations have in place, that would assist too.

Regards,

s 47F

SPORT INTEGRITY AUSTRALIA

Senior Lawyer

Sport Integrity Australia

s 47F **Hotline** 13 000 27232

PO Box 1744, Fyshwick, ACT, 2609 | Unit 14, 5 Tennant St, Fyshwick ACT 2609

PROTECTING SPORT TOGETHER | **sportintegrity.gov.au** |

ACKNOWLEDGEMENT OF COUNTRY

In the spirit of reconciliation we acknowledge the Traditional Custodians of Country throughout Australia and their connections to land, sea and community. We pay our respect to their Elders past, present and future and extend that respect to all Aboriginal and Torres Strait Islander peoples. We recognise the outstanding contribution Aboriginal and Torres Strait Islander peoples make to sport in Australia and celebrate the power of sport to promote reconciliation and reduce inequality.

OFFICIAL: Sensitive

Australian Government
Sport Integrity Australia

SPORT INTEGRITY AUSTRALIA

OAIC

Threshold assessment template

Project Details

Project name	
Date	
Project manager	
Threshold assessment drafter	
Description of the project	
Describe the types of personal information being handled as part of the project	
Is there legal authority for the proposed information handling activity?	
Stakeholders	

Part 1: Does the project or initiative involve new or changed ways of handling personal information?

☐ Yes Complete Part 2 of the assessment below.

☐ No It is not necessary to complete a PIA. Record the decision at Part 3 below and file this assessment with your privacy officer.

Part 2: Determining whether there is the potential for a high privacy risk

Consider the following questions and record each answer as 'yes' or 'no'. The purpose of these questions is to you help you screen for factors which point to the potential for a high privacy risk project. It is important to note that these questions are non-exhaustive, and you should also consider whether there are any other relevant factors that may indicate that your project has the potential to be a high privacy risk project.

Will the project involve:	**Yes**	**No**
Handling large amounts of personal information? *Consider the amount of personal information and the number of individuals that will be impacted by your project. Even if you consider that each individual will only have a small chance of suffering a negative impact, handling personal information on a large scale can increase the privacy risk associated with your project. You should also consider whether your project will result in significant increases in the volume of personal information being handled through new or existing channels.*	☐	☐
Handling sensitive information? *Sensitive information includes, but is not limited to, information about an individual's racial or ethnic origin, political opinions, religious beliefs or affiliations, criminal records, sexual orientation or practices, biometric information[1], health information and genetic information.* *The privacy risk associated with your project can increase if sensitive information is involved given the potential for adverse consequences for an individual, or those associated with the individual, if it is*	☐	☐

[1] Biometric information is an electronic copy of an individual's face, fingerprints, iris, palm, signature or voice.

Will the project involve:	Yes	No
mishandled (for example, discrimination, mistreatment, humiliation or embarrassment).		
Sensitivities based on the context in which the project will operate? *Consider the context and circumstances surrounding the project. Are there prior concerns over this type of handling or activity? Is the project likely to have community support? Is the handling of personal information novel in any way? What is the current state of technology in this area and has there been any previously identified security or technology flaws? Are there any current issues of public concern that you should factor in? What is the nature of your relationship with individuals that may be impacted by the project? How much control will they have over the handling of their personal information? Would they expect you to use their personal information in this way?*	☐	☐
Handling personal information of individuals with particular needs? *Consider whether the activity may have greater sensitivities or disproportionate impacts on certain populations or groups of individuals. This could include children and seniors, people with impaired intellectual or physical functioning, people who are not native speakers of the local language, people with low levels of literacy or education, people from a low socio-economic background, people experiencing financial hardship, people who are Aboriginal or Torres Strait Islanders.* *An individual's circumstances, or the increased power imbalance between the individual and an agency, may mean, for example, they are unable to easily consent to, or oppose, the handling of their personal information, understand its implications, or exercise control over their personal information.*	☐	☐
Handling personal information in a way that could have a significant impact on the individuals concerned? *Consider the potential consequences for the individuals concerned. For example, negative impacts on physical and mental wellbeing, reduced access to public services, discrimination, financial loss or identity theft. Also consider whether the project has a significant collective impact on society, for example, increased surveillance and monitoring activities or the establishment of sensitive personal information sharing arrangements between the Commonwealth and other entities.*	☐	☐

Activity-based risk factors

Will the project involve:	Yes	No
Using or disclosing personal information for secondary purposes? *A 'secondary purpose' is any purpose other than the primary purpose for which the APP entity collected the personal information.*	☐	☐
Disclosing personal information outside of your agency? *Consider whether your project will involve sharing personal information with another agency, organisation or to any individuals other than the individual to whom the information relates. This might include the use of contractors or sub-contractors. Also consider whether your project will require the disclosure of personal information overseas or to an overseas-based company.*	☐	☐
Using or disclosing personal information for profiling or behavioural predictions? *This includes valuation or scoring, profiling and predicting (including in relation to economic situation, health, personal preferences or interests, reliability or behaviour, location or movements).*	☐	☐
Using personal information for automated decision-making? *This might include the use of artificial intelligence technologies or data analytics techniques on personal information to produce insights for policy-making or improved service delivery. It might also include using automated decision-making to make decisions that affect the rights, entitlements and opportunities of an individual.*	☐	☐
Systematic monitoring or tracking of individuals? *For example, the introduction or enhancement of a surveillance system, the monitoring of communications, tracking an individual's geolocation or behaviour.*	☐	☐
Collecting personal information without notification to, or consent of, the individual? *This might include collecting personal information about an individual from a third party without the individual's knowledge or consent. It might also include collecting personal information compulsorily under an existing, or proposed, legislative authority.*	☐	☐

Will the project involve:	Yes	No
Data matching or data linkage? *For example, a new data matching program combining, comparing or matching personal information obtained from multiple sources or a data linkage[2] project where information about the same person from different sources is brought together to create a unified dataset.*	☐	☐
Developing legislation to modify the operation of one or more APPs or which seeks to rely on the required or authorised by law exception to the APPs? *This might include legislation or delegated legislation that seeks to modify the operation of one or more APPs in certain circumstances. It might also include legislation that seeks to rely on the required or authorised an exception to the APPs (such as legislation authorising the use or disclosure of personal information).*	☐	☐

Part 3: Decision & declaration

If you have answered 'Yes' to any of the questions in Part 2, a PIA is likely to be required. If you are uncertain as to whether a PIA is required, you are strongly encouraged to seek support from your agency's privacy officer to ensure your assessment is thorough and complete. If still unsure, err on the side of caution and conduct a PIA.

Based on your answers above, is a PIA required?

☐ Yes Yes, a PIA is required.

☐ No No, a PIA is not required.

[2] Data linkage may also be referred to as 'data integration'.

Outline why it is not necessary to complete a PIA. This may be because the project does not involve personal information (for example, de-identified data is being used) or the project does not involve a new or changed way of handling personal information (refer to your assessment at Part 1 above). If the project is not new, you could include a description of how privacy risks have previously been assessed and are being managed.

If you have ticked one of the boxes in Part 2 above, but have determined that a PIA is not necessary, outline your reasons why. It is the responsibility of each agency to be able to justify why a new or changed way of handling personal information does not have the potential to be high privacy risk.

Assessor Sign-off

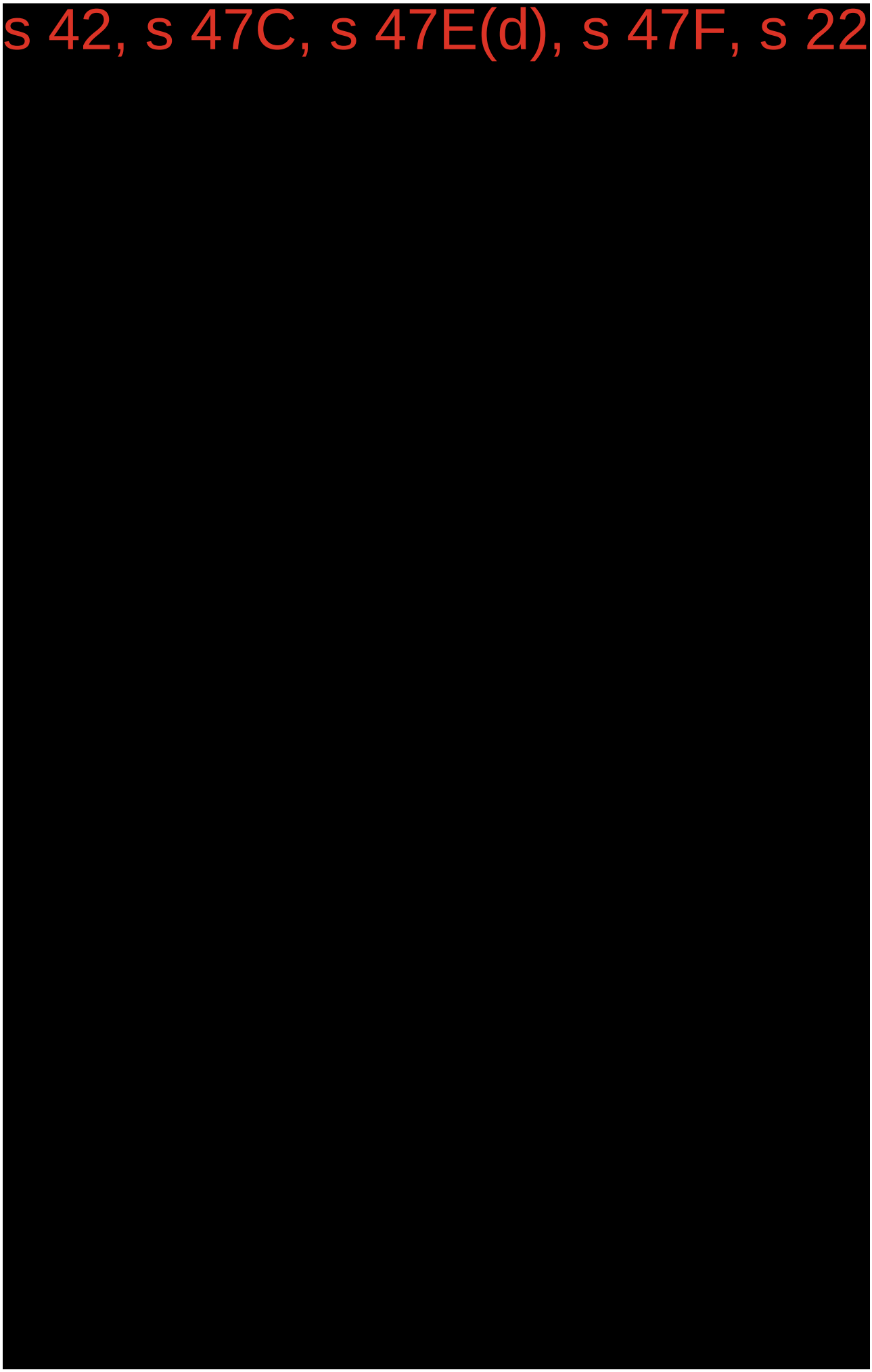
Name	Position	Date

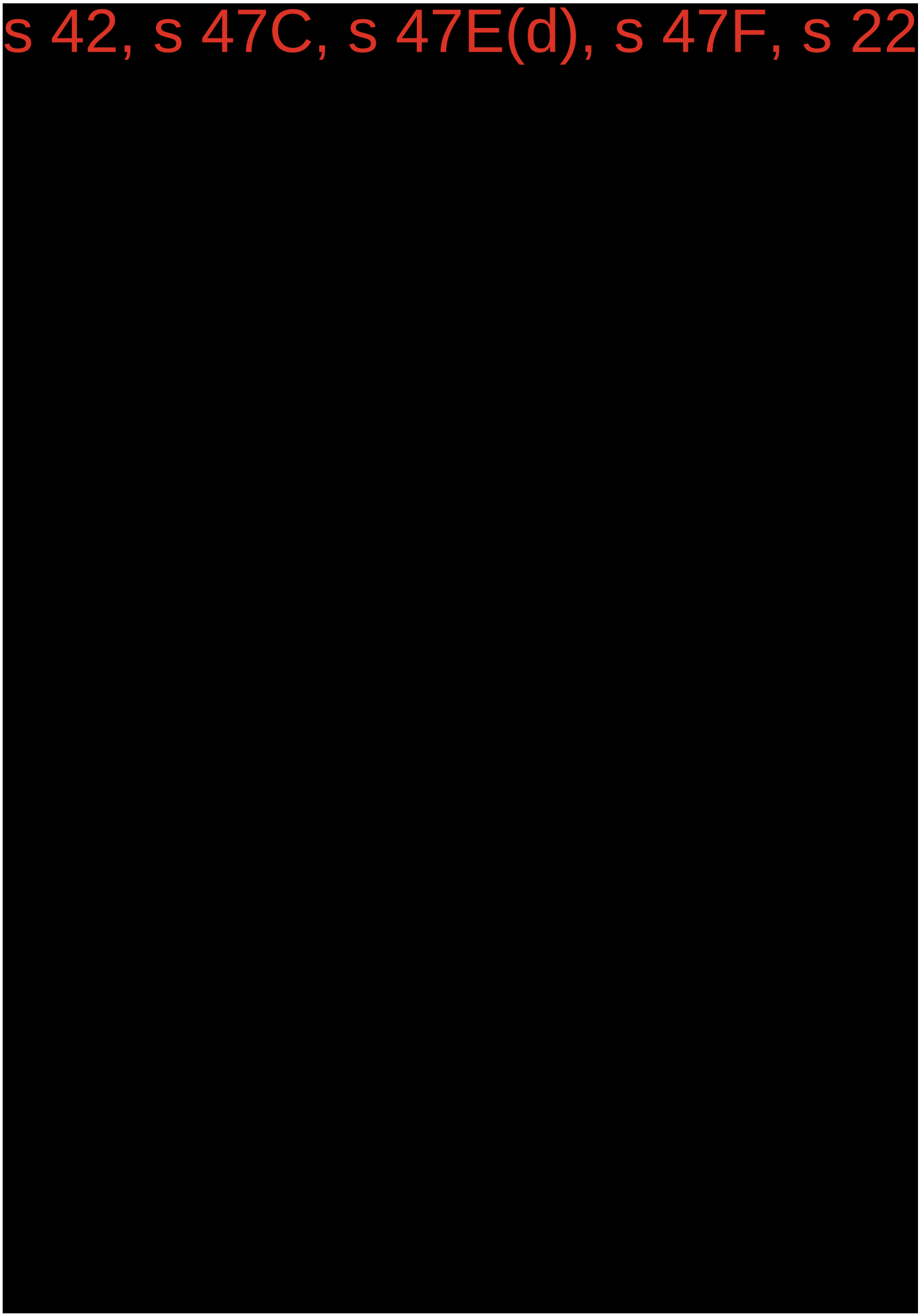
Approver Sign-off

Name	Position	Date

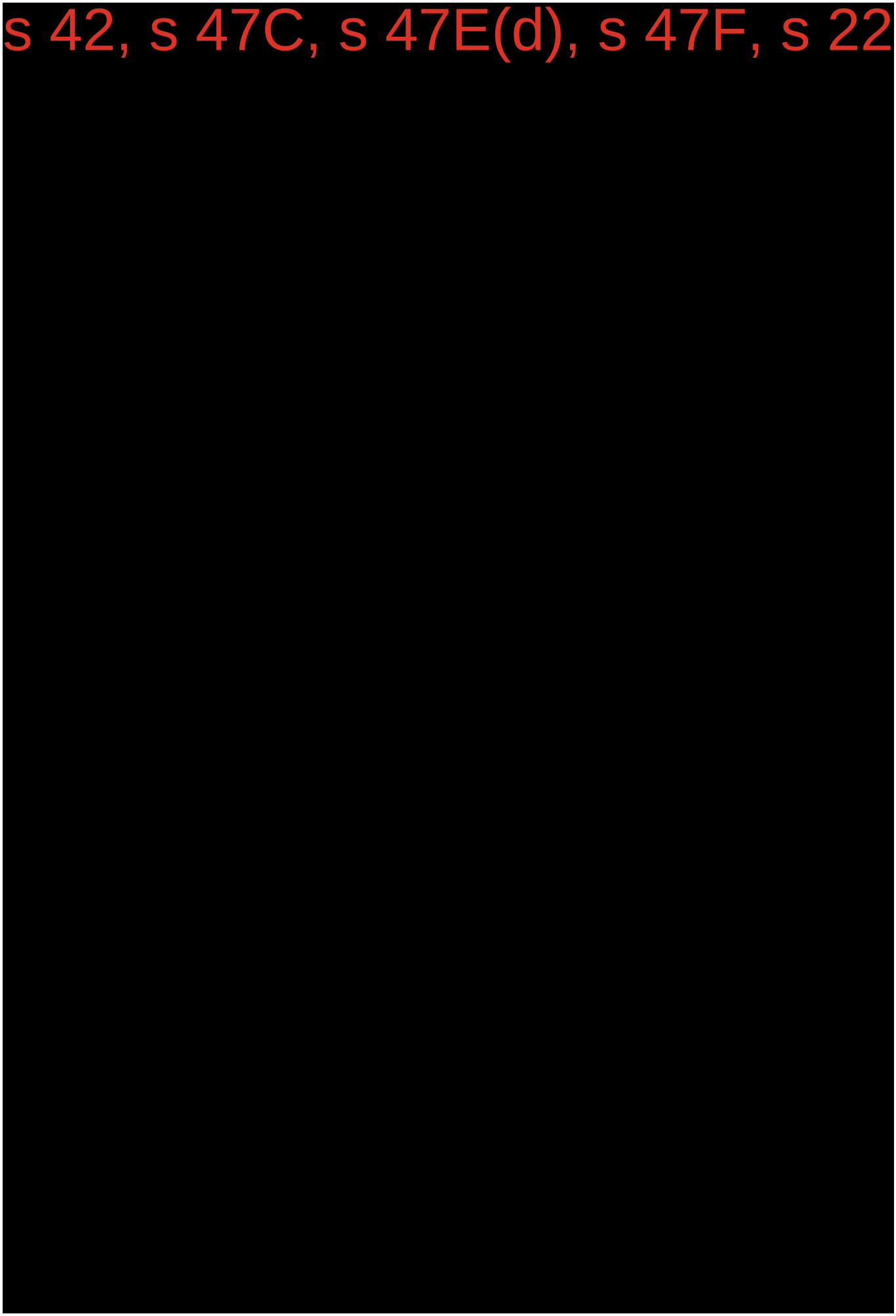
Privacy Officer Sign-off

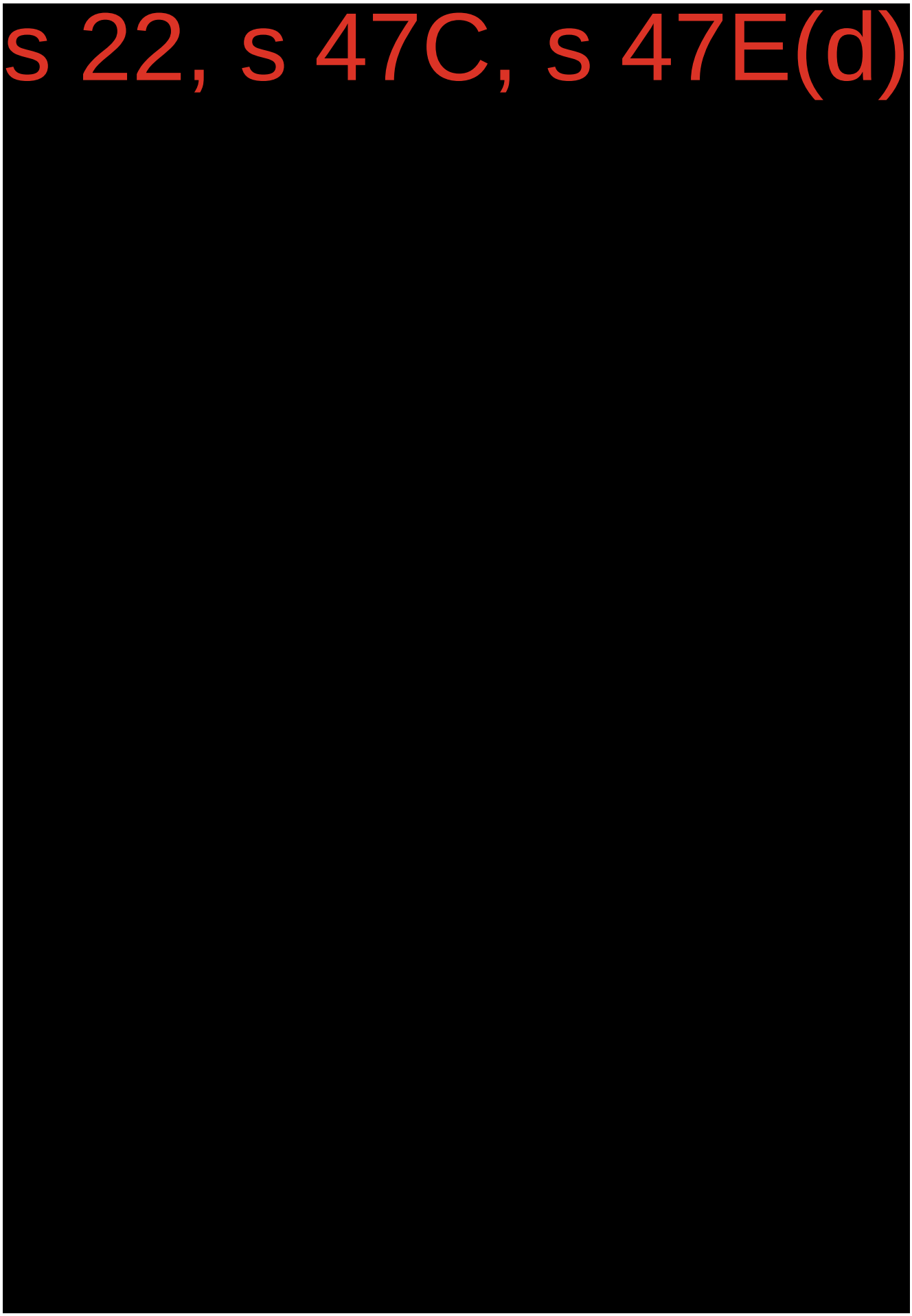
Name	Date


s 42, s 47C, s 47E(d), s 47F, s 22


s 42, s 47C, s 47E(d), s 47F, s 22

s 42, s 47C, s 47E(d), s 47F, s 22


s 42, s 47C, s 47E(d), s 47F, s 22


s 22, s 47C, s 47E(d)

Australian Government
Sport Integrity Australia

SPORT INTEGRITY AUSTRALIA

OAIC

Threshold assessment template

Project Details

Project name	
Date	
Project manager	
Threshold assessment drafter	
Description of the project	*Include a brief description of the project including whether it is a new or existing project. If it is an existing project, describe the proposed changes to the personal information handling practices. You may wish to include links to more detailed project documentation.*
Describe the types of personal information being handled as part of the project	*Brief description of the personal information that will be handled (including personal information that will be collected, used or disclosed, stored, destroyed, de-identified).*
Is there legal authority for the proposed information handling activity?	*Is there legal authority for the proposed information handling activity (for example, is there an existing law that authorises the collection, use or disclosure of personal information for the purposes of the project)? Are there any secrecy provisions that may apply to the proposed information handling activity? Does the information handling activity align with your agency's functions and activities?*
Stakeholders	*List the internal and external stakeholders who have an interest in, or will be affected by, the project. It may be necessary to consult with other areas within your agency, partner agencies or other organisations. You may also approach your agency's Privacy Officer for assistance with completing a threshold assessment or to discuss the project's approach to personal information handling.*

Part 1: Does the project or initiative involve new or changed ways of handling personal information?

☐ Yes Complete Part 2 of the assessment below.

☐ No It is not necessary to complete a PIA. Record the decision at Part 3 below and file this assessment with your privacy officer.

Part 2: Determining whether there is the potential for a high privacy risk

Consider the following questions and record each answer as 'yes' or 'no'. The purpose of these questions is to you help you screen for factors which point to the potential for a high privacy risk project. It is important to note that these questions are non-exhaustive, and you should also consider whether there are any other relevant factors that may indicate that your project has the potential to be a high privacy risk project.

Will the project involve:	**Yes**	**No**
Handling large amounts of personal information? *Consider the amount of personal information and the number of individuals that will be impacted by your project. Even if you consider that each individual will only have a small chance of suffering a negative impact, handling personal information on a large scale can increase the privacy risk associated with your project. You should also consider whether your project will result in significant increases in the volume of personal information being handled through new or existing channels.*	☐	☐
Handling sensitive information? *Sensitive information includes, but is not limited to, information about an individual's racial or ethnic origin, political opinions, religious beliefs or affiliations, criminal records, sexual orientation or practices, biometric information[1], health information and genetic information.* *The privacy risk associated with your project can increase if sensitive information is involved given the potential for adverse consequences for an individual, or those associated with the individual, if it is*	☐	☐

[1] Biometric information is an electronic copy of an individual's face, fingerprints, iris, palm, signature or voice.

Will the project involve:	Yes	No
mishandled (for example, discrimination, mistreatment, humiliation or embarrassment).		
Sensitivities based on the context in which the project will operate? *Consider the context and circumstances surrounding the project. Are there prior concerns over this type of handling or activity? Is the project likely to have community support? Is the handling of personal information novel in any way? What is the current state of technology in this area and has there been any previously identified security or technology flaws? Are there any current issues of public concern that you should factor in? What is the nature of your relationship with individuals that may be impacted by the project? How much control will they have over the handling of their personal information? Would they expect you to use their personal information in this way?*	☐	☐
Handling personal information of individuals with particular needs? *Consider whether the activity may have greater sensitivities or disproportionate impacts on certain populations or groups of individuals. This could include children and seniors, people with impaired intellectual or physical functioning, people who are not native speakers of the local language, people with low levels of literacy or education, people from a low socio-economic background, people experiencing financial hardship, people who are Aboriginal or Torres Strait Islanders.* *An individual's circumstances, or the increased power imbalance between the individual and an agency, may mean, for example, they are unable to easily consent to, or oppose, the handling of their personal information, understand its implications, or exercise control over their personal information.*	☐	☐
Handling personal information in a way that could have a significant impact on the individuals concerned? *Consider the potential consequences for the individuals concerned. For example, negative impacts on physical and mental wellbeing, reduced access to public services, discrimination, financial loss or identity theft. Also consider whether the project has a significant collective impact on society, for example, increased surveillance and monitoring activities or the establishment of sensitive personal information sharing arrangements between the Commonwealth and other entities.*	☐	☐

Activity-based risk factors

Will the project involve:	Yes	No
Using or disclosing personal information for secondary purposes? *A 'secondary purpose' is any purpose other than the primary purpose for which the APP entity collected the personal information.*	☐	☐
Disclosing personal information outside of your agency? *Consider whether your project will involve sharing personal information with another agency, organisation or to any individuals other than the individual to whom the information relates. This might include the use of contractors or sub-contractors. Also consider whether your project will require the disclosure of personal information overseas or to an overseas-based company.*	☐	☐
Using or disclosing personal information for profiling or behavioural predictions? *This includes valuation or scoring, profiling and predicting (including in relation to economic situation, health, personal preferences or interests, reliability or behaviour, location or movements).*	☐	☐
Using personal information for automated decision-making? *This might include the use of artificial intelligence technologies or data analytics techniques on personal information to produce insights for policy-making or improved service delivery. It might also include using automated decision-making to make decisions that affect the rights, entitlements and opportunities of an individual.*	☐	☐
Systematic monitoring or tracking of individuals? *For example, the introduction or enhancement of a surveillance system, the monitoring of communications, tracking an individual's geolocation or behaviour.*	☐	☐
Collecting personal information without notification to, or consent of, the individual? *This might include collecting personal information about an individual from a third party without the individual's knowledge or consent. It might also include collecting personal information compulsorily under an existing, or proposed, legislative authority.*	☐	☐

Will the project involve:	Yes	No
Data matching or data linkage? *For example, a new data matching program combining, comparing or matching personal information obtained from multiple sources or a data linkage[2] project where information about the same person from different sources is brought together to create a unified dataset.*	☐	☐
Developing legislation to modify the operation of one or more APPs or which seeks to rely on the required or authorised by law exception to the APPs? *This might include legislation or delegated legislation that seeks to modify the operation of one or more APPs in certain circumstances. It might also include legislation that seeks to rely on the required or authorised an exception to the APPs (such as legislation authorising the use or disclosure of personal information).*	☐	☐

Part 3: Decision & declaration

If you have answered 'Yes' to any of the questions in Part 2, a PIA is likely to be required. If you are uncertain as to whether a PIA is required, you are strongly encouraged to seek support from your agency's privacy officer to ensure your assessment is thorough and complete. If still unsure, err on the side of caution and conduct a PIA.

Based on your answers above, is a PIA required?

☐ Yes Yes, a PIA is required.

☐ No No, a PIA is not required.

[2] Data linkage may also be referred to as 'data integration'.

Outline why it is not necessary to complete a PIA. This may be because the project does not involve personal information (for example, de-identified data is being used) or the project does not involve a new or changed way of handling personal information (refer to your assessment at Part 1 above). If the project is not new, you could include a description of how privacy risks have previously been assessed and are being managed.

If you have ticked one of the boxes in Part 2 above, but have determined that a PIA is not necessary, outline your reasons why. It is the responsibility of each agency to be able to justify why a new or changed way of handling personal information does not have the potential to be high privacy risk.

Assessor Sign-off

Name	Position	Date

Approver Sign-off

Name	Position	Date

Privacy Officer Sign-off

Name	Date

Outlook

Fw: FW: Privacy Impact Assessment - information [SEC=OFFICIAL]

s 47F

Date Fri 08-May-2026 2:10 PM

s 47F

10 attachments (385 KB)

Threshold assessment template.docx; Draft - SIA Privacy Manual - March 2023.docx; image001.jpg; image002.jpg; image004.jpg; image006.jpg; image008.jpg; image009.jpg; image010.jpg; image011.jpg;

---

s 47F

Sent: Thursday, November 09, 2023 9:59 AM

s 47F

Subject: Fw: FW: Privacy Impact Assessment - information

OFFICIAL: Sensitive

s 47F here is the threshold assessment template we discussed yesterday (to determine if a PIA is required).

This should be done by the business area.

Regards,

s 47F
Senior Lawyer | Legal
SPORT INTEGRITY AUSTRALIA
s 47F **Hotline** 13 000 27232
PO Box 1744, Fyshwick, ACT, 2609 | Unit 14, 5 Tennant St, Fyshwick ACT 2609
PROTECTING SPORT TOGETHER | **sportintegrity.gov.au** |

ACKNOWLEDGEMENT OF COUNTRY

In the spirit of reconciliation we acknowledge the Traditional Custodians of Country throughout Australia and their connections to land, sea and community. We pay our respect to their Elders past, present and future and extend that respect to all Aboriginal and Torres Strait Islander peoples. We recognise the outstanding contribution Aboriginal and Torres Strait Islander peoples make to sport in Australia and celebrate the power of sport to promote reconciliation and reduce inequality.

OFFICIAL: Sensitive

s 47F

Sent: Wednesday, April 5, 2023 2:22 PM

To: Sarah Benson <Sarah.Benson@sportintegrity.gov.au >
s 47F SIA - Privacy <privacy@sportintegrity.gov.au >
Subject: Privacy Impact Assessment - information

Hi Sarah,

s 47F has asked me to provide you with some information regarding the process of Privacy Impact Assessments within the agency.

We are currently finalising a suite of privacy policies and documents that will assist staff in understanding their privacy obligations. In terms of Privacy Impact Assessments, the draft Privacy Manual at page 11 (copy **attached**) states:

> **Privacy Impact Assessments**
>
> The Privacy Code requires us to undertake a Privacy Impact Assessment (PIA) for all 'high privacy risk ' projects or initiatives that involve new or changed ways of handling personal information. A project will be 'high risk ' if it is likely to have a significant impact on the privacy of individuals.
>
> When developing a project that involves new or changed personal information handling practices, you must advise your managers and conduct a privacy threshold assessment (PTA) to determine whether a PIA should be conducted. You should also engage the Privacy Officer during the planning phase.
>
> Undertaking a PIA is one way in which we can ensure it has regard to privacy risks of a new project or initiative in the development and implementation stages. This means that we not only maintain best practice in collecting and handling personal information, but also we reduce the likelihood of any data or privacy breaches by considering ways of managing, minimising or eliminating any impacts on privacy.
>
> ...

I have **attached** a threshold assessment template, which is the first step to determine whether a PIA should be conducted.

s 22, s 38, s 47E(d), s 42

Please let me know if you have any questions or want to discuss.

Regards,

s 47F
Senior Lawyer | Legal
s 47F **Hotline** 13 000 27232
SPORT INTEGRITY AUSTRALIA
PO Box 1744, Fyshwick, ACT, 2609 | Unit 14, 5 Tennant St, Fyshwick ACT 2609
PROTECTING SPORT TOGETHER | **sportintegrity.gov.au** |

ACKNOWLEDGEMENT OF COUNTRY
In the spirit of reconciliation we acknowledge the Traditional Custodians of Country throughout Australia and their connections to land, sea and community. We pay our respect to their Elders past, present and future and extend that respect to all Aboriginal and Torres Strait Islander peoples. We recognise the outstanding contribution Aboriginal and Torres Strait Islander peoples make to sport in Australia and celebrate the power of sport to promote reconciliation and reduce inequality.

Australian Government
Sport Integrity Australia

SPORT INTEGRITY AUSTRALIA

S 47C

s 47C

s 47C

s 47C

s 47C

s 47C

s 47C

s 47C

s 47C


S 47C


S 47C

s 47C

s 47C

S 47C

s 47C

s 47C

s 47C

S 47C

S 47C

s 47C

s 47C

S 47C


S 47C

S 47C


s 47C

s 47C


s 47C

Australian Government
Sport Integrity Australia

SPORT INTEGRITY AUSTRALIA

OAIC

Threshold assessment template

Project Details

Project name	
Date	
Project manager	
Threshold assessment drafter	
Description of the project	*Include a brief description of the project including whether it is a new or existing project. If it is an existing project, describe the proposed changes to the personal information handling practices. You may wish to include links to more detailed project documentation.*
Describe the types of personal information being handled as part of the project	*Brief description of the personal information that will be handled (including personal information that will be collected, used or disclosed, stored, destroyed, de-identified).*
Is there legal authority for the proposed information handling activity?	*Is there legal authority for the proposed information handling activity (for example, is there an existing law that authorises the collection, use or disclosure of personal information for the purposes of the project)? Are there any secrecy provisions that may apply to the proposed information handling activity? Does the information handling activity align with your agency's functions and activities?*
Stakeholders	*List the internal and external stakeholders who have an interest in, or will be affected by, the project. It may be necessary to consult with other areas within your agency, partner agencies or other organisations. You may also approach your agency's Privacy Officer for assistance with completing a threshold assessment or to discuss the project's approach to personal information handling.*

Part 1: Does the project or initiative involve new or changed ways of handling personal information?

☐ Yes Complete Part 2 of the assessment below.

☐ No It is not necessary to complete a PIA. Record the decision at Part 3 below and file this assessment with your privacy officer.

Part 2: Determining whether there is the potential for a high privacy risk

Consider the following questions and record each answer as 'yes' or 'no'. The purpose of these questions is to you help you screen for factors which point to the potential for a high privacy risk project. It is important to note that these questions are non-exhaustive, and you should also consider whether there are any other relevant factors that may indicate that your project has the potential to be a high privacy risk project.

Will the project involve:	Yes	No
Handling large amounts of personal information? *Consider the amount of personal information and the number of individuals that will be impacted by your project. Even if you consider that each individual will only have a small chance of suffering a negative impact, handling personal information on a large scale can increase the privacy risk associated with your project. You should also consider whether your project will result in significant increases in the volume of personal information being handled through new or existing channels.*	☐	☐
Handling sensitive information? *Sensitive information includes, but is not limited to, information about an individual's racial or ethnic origin, political opinions, religious beliefs or affiliations, criminal records, sexual orientation or practices, biometric information[1], health information and genetic information.* *The privacy risk associated with your project can increase if sensitive information is involved given the potential for adverse consequences for an individual, or those associated with the individual, if it is*	☐	☐

[1] Biometric information is an electronic copy of an individual's face, fingerprints, iris, palm, signature or voice.

Will the project involve:	Yes	No
mishandled (for example, discrimination, mistreatment, humiliation or embarrassment).		
Sensitivities based on the context in which the project will operate? *Consider the context and circumstances surrounding the project. Are there prior concerns over this type of handling or activity? Is the project likely to have community support? Is the handling of personal information novel in any way? What is the current state of technology in this area and has there been any previously identified security or technology flaws? Are there any current issues of public concern that you should factor in? What is the nature of your relationship with individuals that may be impacted by the project? How much control will they have over the handling of their personal information? Would they expect you to use their personal information in this way?*	☐	☐
Handling personal information of individuals with particular needs? *Consider whether the activity may have greater sensitivities or disproportionate impacts on certain populations or groups of individuals. This could include children and seniors, people with impaired intellectual or physical functioning, people who are not native speakers of the local language, people with low levels of literacy or education, people from a low socio-economic background, people experiencing financial hardship, people who are Aboriginal or Torres Strait Islanders.* *An individual's circumstances, or the increased power imbalance between the individual and an agency, may mean, for example, they are unable to easily consent to, or oppose, the handling of their personal information, understand its implications, or exercise control over their personal information.*	☐	☐
Handling personal information in a way that could have a significant impact on the individuals concerned? *Consider the potential consequences for the individuals concerned. For example, negative impacts on physical and mental wellbeing, reduced access to public services, discrimination, financial loss or identity theft. Also consider whether the project has a significant collective impact on society, for example, increased surveillance and monitoring activities or the establishment of sensitive personal information sharing arrangements between the Commonwealth and other entities.*	☐	☐

Activity-based risk factors

Will the project involve:	Yes	No
Using or disclosing personal information for secondary purposes? *A 'secondary purpose' is any purpose other than the primary purpose for which the APP entity collected the personal information.*	☐	☐
Disclosing personal information outside of your agency? *Consider whether your project will involve sharing personal information with another agency, organisation or to any individuals other than the individual to whom the information relates. This might include the use of contractors or sub-contractors. Also consider whether your project will require the disclosure of personal information overseas or to an overseas-based company.*	☐	☐
Using or disclosing personal information for profiling or behavioural predictions? *This includes valuation or scoring, profiling and predicting (including in relation to economic situation, health, personal preferences or interests, reliability or behaviour, location or movements).*	☐	☐
Using personal information for automated decision-making? *This might include the use of artificial intelligence technologies or data analytics techniques on personal information to produce insights for policy-making or improved service delivery. It might also include using automated decision-making to make decisions that affect the rights, entitlements and opportunities of an individual.*	☐	☐
Systematic monitoring or tracking of individuals? *For example, the introduction or enhancement of a surveillance system, the monitoring of communications, tracking an individual's geolocation or behaviour.*	☐	☐
Collecting personal information without notification to, or consent of, the individual? *This might include collecting personal information about an individual from a third party without the individual's knowledge or consent. It might also include collecting personal information compulsorily under an existing, or proposed, legislative authority.*	☐	☐

Will the project involve:	Yes	No
Data matching or data linkage? *For example, a new data matching program combining, comparing or matching personal information obtained from multiple sources or a data linkage[2] project where information about the same person from different sources is brought together to create a unified dataset.*	☐	☐
Developing legislation to modify the operation of one or more APPs or which seeks to rely on the required or authorised by law exception to the APPs? *This might include legislation or delegated legislation that seeks to modify the operation of one or more APPs in certain circumstances. It might also include legislation that seeks to rely on the required or authorised an exception to the APPs (such as legislation authorising the use or disclosure of personal information).*	☐	☐

Part 3: Decision & declaration

If you have answered 'Yes' to any of the questions in Part 2, a PIA is likely to be required. If you are uncertain as to whether a PIA is required, you are strongly encouraged to seek support from your agency's privacy officer to ensure your assessment is thorough and complete. If still unsure, err on the side of caution and conduct a PIA.

Based on your answers above, is a PIA required?

☐ Yes Yes, a PIA is required.

☐ No No, a PIA is not required.

[2] Data linkage may also be referred to as 'data integration'.

Outline why it is not necessary to complete a PIA. This may be because the project does not involve personal information (for example, de-identified data is being used) or the project does not involve a new or changed way of handling personal information (refer to your assessment at Part 1 above). If the project is not new, you could include a description of how privacy risks have previously been assessed and are being managed.

If you have ticked one of the boxes in Part 2 above, but have determined that a PIA is not necessary, outline your reasons why. It is the responsibility of each agency to be able to justify why a new or changed way of handling personal information does not have the potential to be high privacy risk.

Assessor Sign-off

Name	Position	Date

Approver Sign-off

Name	Position	Date

Privacy Officer Sign-off

Name	Date

SIA Corporate Services
Privacy Impact Statement

Version 1.0

Terms of Reference

Users	Sport Integrity Australia Employees, excluding casual staff (Chaperones)
PI	Personal Information which **can** include sensitive Personal Information
The app(s)	The SIA Corporate Services Application
IPO Report	Information of Position Occupant Report

Privacy Impact Assessment

Project Summary

The SIA Corporate Services (the app) is Microsoft PowerApps application that unifies internal workflows by integrating processes from Finance, Human Resources, ICT Property and Security, and Travel into a single, centralised location. Currently, these processes operate independently and inconsistently, and fragment access to data.

By consolidating these processes into one central user-friendly interface, the app provides a more efficient and consistent experience for staff.

The application includes the following workflows:

- Conflict of interest
- International travel approval flows
- Finance spending proposals
- Outside employment
- Incident reporting
- IT service desk

The app is expected to include additional workflows such as Gift and Benefit declarations, flexible working arrangement applications, and more.

The current build of the project utilises SharePoint Lists and its inbuilt security features to store and record information. In combination with Microsoft Power Automate, SharePoint Lists provide row level security to manage access to records.

Whilst the current solution satisfies baseline privacy requirements, additional funding for the implementation of PowerApps Premium would further strengthen security controls to Personal Information (PI) and provide a scalable relational database.

The app is developed and maintained by the ICT Team and enables key stakeholders within the agency to automate their workflows.

Scope of Impact Assessment

This PIA considers the stakeholders, information, and components and processes relevant to the app.

Stakeholders

SIA and SIA staff who are required to complete governance disclosures and declarations. As a Federal Government Agency, these attestations are crucial in allowing SIA to maintain its integrity and compliance with the APS Code of Conduct.

Information

The app manages and stores the PI of staff which in some cases may be sensitive PI. This may include personal/contact details, identifiers such as AGS, health information, accessibility requirements, workplace incidents, and conflict information.

Components and Processes

The Microsoft Power Platform hosts the application and stores the information within SIAs Microsoft Tenancy. The app uses Power Apps and Power Automate to present, and manage information, and uses SharePoint to store information.

Whilst the app provides a medium for which to modify and store information. The use and disclosure of PI remains with the workflow owners; where applicable, workflow owners may apply their own Privacy Policies and practices in line with their requirements.

This PIA does not assess the impact and security of legacy and deprecated systems and does not extend to major future changes or system redesigns, which should be considered separately.

System Information Flow

Information which is submitted by users is handled and processed by Power Automate. Power Automate allows for access control to records to be automatically applied to relevant staff. Data stored in SharePoint can be accessed through the app and directly through SharePoint which determines access rights to records.

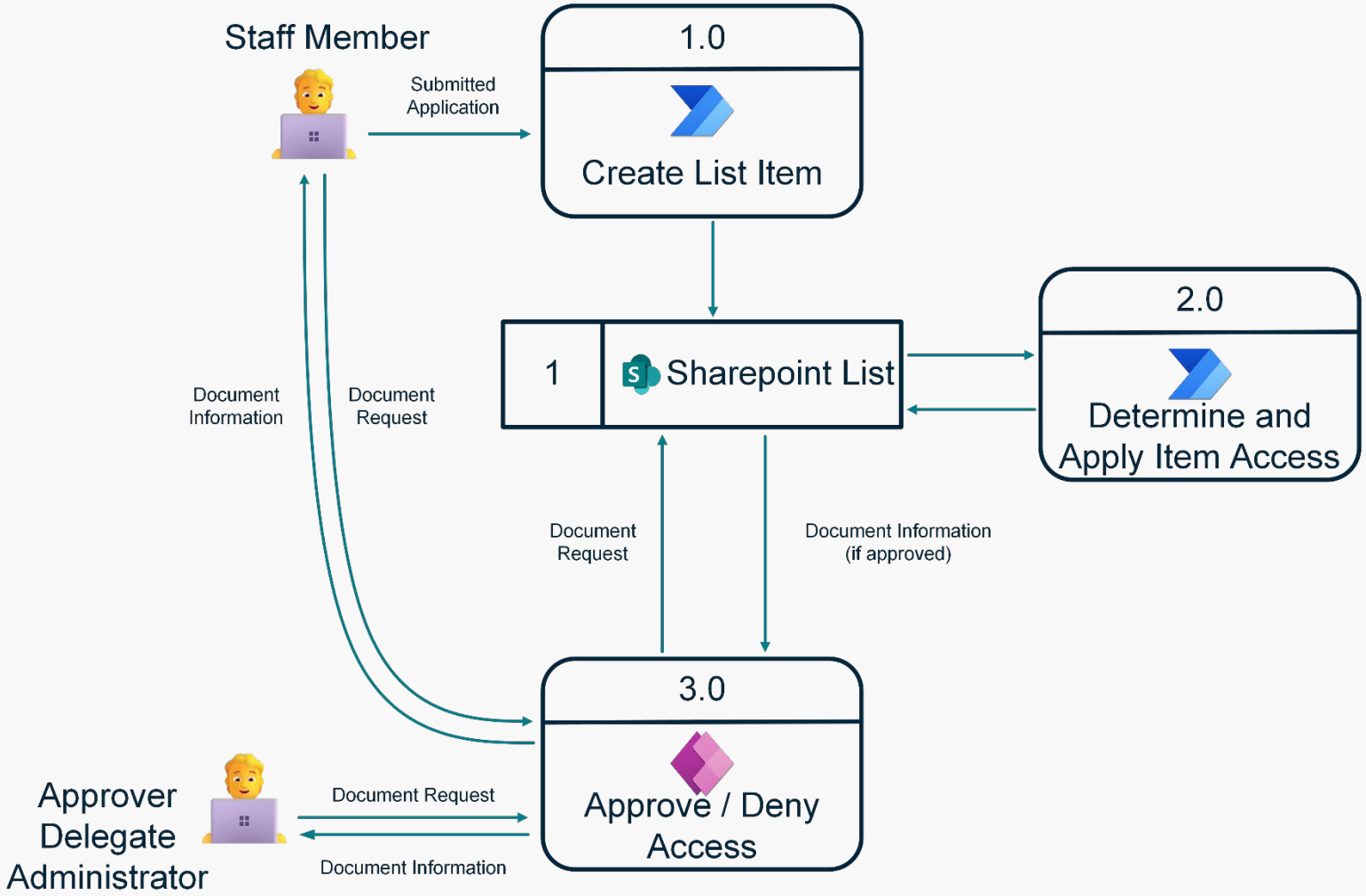


Figure 1.0 – High Level Data Flow Diagram of The App

Privacy Impact and Compliance Analysis

Privacy Risks

The following privacy risks have been identified:

Unauthorised Access to Personal Information

Unauthorised access to sensitive PI may occur in cases where misconfigured SharePoint access is applied. Delayed or incorrect IPO data may also lead to unauthorised access, as access to records is determined by position numbers obtained from the SAP IPO report.

Data Leakage through Integrations

Integrations such as Power Automate may in some cases fetch data automatically when information is created in SharePoint. This may result in an individual collecting data with automation which they should not be permitted to access.

Inability to audit log access

Microsoft Lists does not have the ability to collect logs on viewed information and viewed lists. This means that there is no detailed information which shows user access to specific lists and records.

Exposure

The exposure of information by staff to third parties is a potential risk. These third parties can include and are not limited to unauthorised staff, non-affiliated individuals/entities, and external platforms/digital services.

Privacy Impact Analysis

Whilst the apps' purpose is to provide a platform to allow staff to view and manage PI, the collection of this information is necessary due to SIAs requirement as an employer and Federal Government Agency. The method of collection differs to the current workflows; however, the use and disclosure of PI remains the same.

The app automates and unifies current corporate workflows and does not develop new uses and applications of PI.

As the use and disclosure of PI remains the same, the apps collection of PI aligns with stakeholder expectations and privacy values.

Australian Privacy Principal Relations

To ensure compliance with the APP the following steps have been taken:

APP 1

A privacy policy for users of the app has been written and will be made available to staff. (Please see appendix A.1 for the privacy policy).

This policy will be updated should new workflows, modifications to workflows, or major updates to the apps components and/or processes be developed. Contacts for staff to make inquiries and complaints is included should they be required.

APP 2

Not applicable as the applications purpose is to store information regarding staff and their employment.

APP 3

The collection of PI is required and is necessary for the purposes of the app.

The following PI is stored in SharePoint:

- Staff information
- Staff conflict details
- Conflict management plans
- Travel accessibility requirements
- Staff Outside employment details, employer and position details
- Workplace incident details, including staff involved and details of the incident.
- Flexible working arrangements including details and justification for arrangements.

Staff provide required personal information (required under the APS Code of Conduct) to SIA to satisfy the agencies functions, activities, and requirements as a Federal Government Agency.

Personal Information about an individual which is not provided by the individual is collected in cases where SIA is authorised and required as an employer to record certain attestations.

APP 4

There may be cases where an employee submits sensitive PI in relation to another employee such as in the case of workplace incidents. This information can be collected as outlined under APP 3 above.

Destruction or deidentification of this information may not be reasonable as under Work Health and Safety regulation, employees are required to report incidents such as physical and/or psychological hazards occurring within the workplace.

PI which does not satisfy APP 3 and meets APP 4.3, can be deleted by the ICT, Property and Security team, or by the workflow administrators.

APP 5

Information collected by workflow owners is subject to their information privacy policies, and as such, the processes and procedures relating to the notification of collection of PI is subject to the respective workflow privacy policies.

APP 6

The PI disclosed is used by the relevant teams and staff who own and are required to act in the specific workflows, and the information is subject to the respective privacy policies.

APP 7

Not applicable as PI disclosed is not used for marketing.

APP 8

Not applicable as PI is not disclosed overseas.

APP 9

The use of a government related identifier (AGS Number) may in some cases be required and is permitted under APP 9.24 (An organisation may use or disclose the government related identifier of an individual if the use or disclosure is reasonably necessary for the organisation to verify the identity of the individual for the purposes of the organisation's activities or functions (APP 9.2(a)).)

APP 10

Information entered into the app should adhere to APS Code of Conduct. Should information be inaccurate and require correction, users of the app can amend and update PI, alternatively, ICT can amend and correct information in cases where users are restricted from making changes to information.

APP 11

Reasonable steps are taken to protect PI; Microsoft access controls provide relevant parties (i.e. PI Creator, approvers, delegates and/or workflow administrators) with access to specific records. Version history is available allowing record changes to be recorded.

APP 12

Access to PI is available to staff to which the PI relates and can be determined by workflow privacy policies. Access may be adjusted due to Position Occupant changes.

APP 13

Information can be corrected and amended should this be required. Staff can contact HR and ICT to correct information should it be incorrect.

Privacy Management assessing the risks

SharePoint lists are configured to (by default) only permit the record creator to access the record. Access is then provided to relevant users by automations which determine access from IPO data. Delays in processing this data may allow previous position occupants to view data no longer relevant to them. Previous position occupants shall maintain visibility over records in which they have made governance actions. Additionally, users can be assigned roles by workflow administrators which permit record access and management; misconfigured or delayed access management may lead to unauthorised access to PI.

Record permissions for users apply to any automations created and owned by users. This mitigates the risk of data leakage through service integrations by only permitting a user to fetch information (through automations) which they would be permitted to view.

Finally, APS Code of Conduct prohibits the improper use, disclosure or handling of official information which includes PI.

Summary of risks

The occurrence of the identified risks occurring from the development and design of the application can be considered low as there are ongoing mitigations and access controls in place aiming to prevent unauthorised access; in addition to these mitigations, Law, Policy and Legislation prevent the misuse and disclosure of PI by the users of the app.

Response to risks

In the case of incorrect access, ICT will immediately, when notified, manually remove access and investigate if the access was granted due to incorrect data or due to an error in the logic of the flows providing viewing access. The result of investigations will inform and direct remediations to prevent and resolve privacy incidents or unintended disclosures of personal information.

In addition to the above, ICT may conduct access audits to ensure information from workflows is available only to relevant staff.

Conclusion

The SIA corporate services application is a centralised corporate governance system that unifies and automates multiple agency attestation workflows. Whilst technologies used may allow for unauthorised access to PI, policy, law, legislation, and mitigations are in place to prevent the misuse and unauthorised disclosure of PI. Future builds of the app that introduce new privacy risks should be subject to separate review.

Overall, the current processes and mitigations are sufficient in protecting the PI of SIA employees. To ensure the continuous protection of PI, ongoing monitoring and audits are recommended to ensure compliance with the apps privacy policy and requirements in handling personal information.

Relevant Legislation, Policies and Guidelines

APS Code of Conduct, Australian Public Service Commission, 2023

Australian Privacy Principles, Office of the Australian Information Commissioner, 2019

Privacy Act 1988 (Cth)

Public Service Act 1999 (Cth)

Appendices

Appendix A

Privacy Policy

The SIA Corporate Services Application (the application) collects and stores information relating to various corporate workflows. These workflows include and are not limited to, Conflict of Interest declarations, Workplace Incidents, Gift and Benefit Declarations and Notification of Outside Employment.

Personal Information submitted in these workflows is stored in SharePoint and shared with the respective workflow teams and any relevant approvers / delegates. Sensitive Personal Information which you mark as 'Private' will only be visible by you and to your selected HR representative.

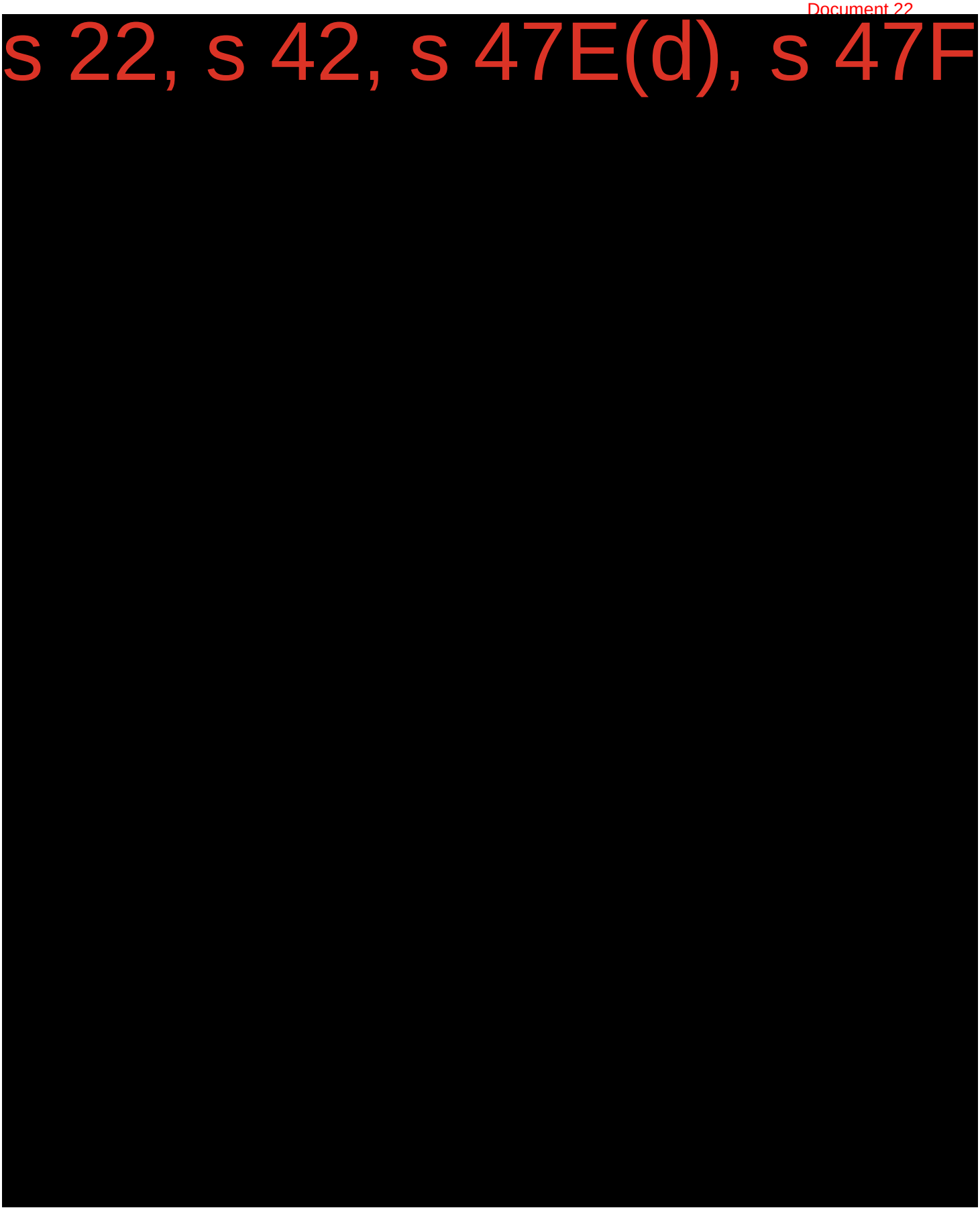
SIA ICT Support may have privileged access to the databases that store your personal information. This access is provided solely for the purpose of maintaining and supporting the application, resolving technical issues, and ensuring the security and integrity of our services.

If you have any concerns, please contact itrequests@sportintegrity.gov.au or humanresources@sportintegrity.gov.au.

s 22, s 42, s 47E(d), s 47F

s 22, s 42, s 47E(d), s 47F

s 22, s 42, s 47E(d), s 47F



Threshold assessment template

Project Details

Project name	
Date	
Project manager	
Threshold assessment drafter	
Description of the project	*Include a brief description of the project including whether it is a new or existing project. If it is an existing project, describe the proposed changes to the personal information handling practices. You may wish to include links to more detailed project documentation.*
Describe the types of personal information being handled as part of the project	*Brief description of the personal information that will be handled (including personal information that will be collected, used or disclosed, stored, destroyed, de-identified).*
Is there legal authority for the proposed information handling activity?	*Is there legal authority for the proposed information handling activity (for example, is there an existing law that authorises the collection, use or disclosure of personal information for the purposes of the project)? Are there any secrecy provisions that may apply to the proposed information handling activity? Does the information handling activity align with your agency's functions and activities?*
Stakeholders	*List the internal and external stakeholders who have an interest in, or will be affected by, the project. It may be necessary to consult with other areas within your agency, partner agencies or other organisations. You may also approach your agency's Privacy Officer for assistance with completing a threshold assessment or to discuss the project's approach to personal information handling.*

Part 1: Does the project or initiative involve new or changed ways of handling personal information?

☐ Yes — Complete Part 2 of the assessment below.

☐ No — It is not necessary to complete a PIA. Record the decision at Part 3 below and file this assessment with your privacy officer.

Part 2: Determining whether there is the potential for a high privacy risk

Consider the following questions and record each answer as 'yes' or 'no'. The purpose of these questions is to you help you screen for factors which point to the potential for a high privacy risk project. It is important to note that these questions are non-exhaustive, and you should also consider whether there are any other relevant factors that may indicate that your project has the potential to be a high privacy risk project.

Will the project involve:	**Yes**	**No**
Handling large amounts of personal information? *Consider the amount of personal information and the number of individuals that will be impacted by your project. Even if you consider that each individual will only have a small chance of suffering a negative impact, handling personal information on a large scale can increase the privacy risk associated with your project. You should also consider whether your project will result in significant increases in the volume of personal information being handled through new or existing channels.*	☐	☐
Handling sensitive information? *Sensitive information includes, but is not limited to, information about an individual's racial or ethnic origin, political opinions, religious beliefs or affiliations, criminal records, sexual orientation or practices, biometric information[1], health information and genetic information.* *The privacy risk associated with your project can increase if sensitive information is involved given the potential for adverse consequences for an individual, or those associated with the individual, if it is*	☐	☐

[1] Biometric information is an electronic copy of an individual's face, fingerprints, iris, palm, signature or voice.

Will the project involve:	Yes	No
mishandled (for example, discrimination, mistreatment, humiliation or embarrassment).		
Sensitivities based on the context in which the project will operate? *Consider the context and circumstances surrounding the project. Are there prior concerns over this type of handling or activity? Is the project likely to have community support? Is the handling of personal information novel in any way? What is the current state of technology in this area and has there been any previously identified security or technology flaws? Are there any current issues of public concern that you should factor in? What is the nature of your relationship with individuals that may be impacted by the project? How much control will they have over the handling of their personal information? Would they expect you to use their personal information in this way?*	☐	☐
Handling personal information of individuals with particular needs? *Consider whether the activity may have greater sensitivities or disproportionate impacts on certain populations or groups of individuals. This could include children and seniors, people with impaired intellectual or physical functioning, people who are not native speakers of the local language, people with low levels of literacy or education, people from a low socio-economic background, people experiencing financial hardship, people who are Aboriginal or Torres Strait Islanders.* *An individual's circumstances, or the increased power imbalance between the individual and an agency, may mean, for example, they are unable to easily consent to, or oppose, the handling of their personal information, understand its implications, or exercise control over their personal information.*	☐	☐
Handling personal information in a way that could have a significant impact on the individuals concerned? *Consider the potential consequences for the individuals concerned. For example, negative impacts on physical and mental wellbeing, reduced access to public services, discrimination, financial loss or identity theft. Also consider whether the project has a significant collective impact on society, for example, increased surveillance and monitoring activities or the establishment of sensitive personal information sharing arrangements between the Commonwealth and other entities.*	☐	☐

Activity-based risk factors

Will the project involve:	Yes	No
Using or disclosing personal information for secondary purposes? *A 'secondary purpose' is any purpose other than the primary purpose for which the APP entity collected the personal information.*	☐	☐
Disclosing personal information outside of your agency? *Consider whether your project will involve sharing personal information with another agency, organisation or to any individuals other than the individual to whom the information relates. This might include the use of contractors or sub-contractors. Also consider whether your project will require the disclosure of personal information overseas or to an overseas-based company.*	☐	☐
Using or disclosing personal information for profiling or behavioural predictions? *This includes valuation or scoring, profiling and predicting (including in relation to economic situation, health, personal preferences or interests, reliability or behaviour, location or movements).*	☐	☐
Using personal information for automated decision-making? *This might include the use of artificial intelligence technologies or data analytics techniques on personal information to produce insights for policy-making or improved service delivery. It might also include using automated decision-making to make decisions that affect the rights, entitlements and opportunities of an individual.*	☐	☐
Systematic monitoring or tracking of individuals? *For example, the introduction or enhancement of a surveillance system, the monitoring of communications, tracking an individual's geolocation or behaviour.*	☐	☐
Collecting personal information without notification to, or consent of, the individual? *This might include collecting personal information about an individual from a third party without the individual's knowledge or consent. It might also include collecting personal information compulsorily under an existing, or proposed, legislative authority.*	☐	☐

Will the project involve:	Yes	No
Data matching or data linkage? *For example, a new data matching program combining, comparing or matching personal information obtained from multiple sources or a data linkage[2] project where information about the same person from different sources is brought together to create a unified dataset.*	☐	☐
Developing legislation to modify the operation of one or more APPs or which seeks to rely on the required or authorised by law exception to the APPs? *This might include legislation or delegated legislation that seeks to modify the operation of one or more APPs in certain circumstances. It might also include legislation that seeks to rely on the required or authorised an exception to the APPs (such as legislation authorising the use or disclosure of personal information).*	☐	☐

Part 3: Decision & declaration

If you have answered 'Yes' to any of the questions in Part 2, a PIA is likely to be required. If you are uncertain as to whether a PIA is required, you are strongly encouraged to seek support from your agency's privacy officer to ensure your assessment is thorough and complete. If still unsure, err on the side of caution and conduct a PIA.

Based on your answers above, is a PIA required?

☐ Yes Yes, a PIA is required.

☐ No No, a PIA is not required.

[2] Data linkage may also be referred to as 'data integration'.

Outline why it is not necessary to complete a PIA. This may be because the project does not involve personal information (for example, de-identified data is being used) or the project does not involve a new or changed way of handling personal information (refer to your assessment at Part 1 above). If the project is not new, you could include a description of how privacy risks have previously been assessed and are being managed.

If you have ticked one of the boxes in Part 2 above, but have determined that a PIA is not necessary, outline your reasons why. It is the responsibility of each agency to be able to justify why a new or changed way of handling personal information does not have the potential to be high privacy risk.

Assessor Sign-off

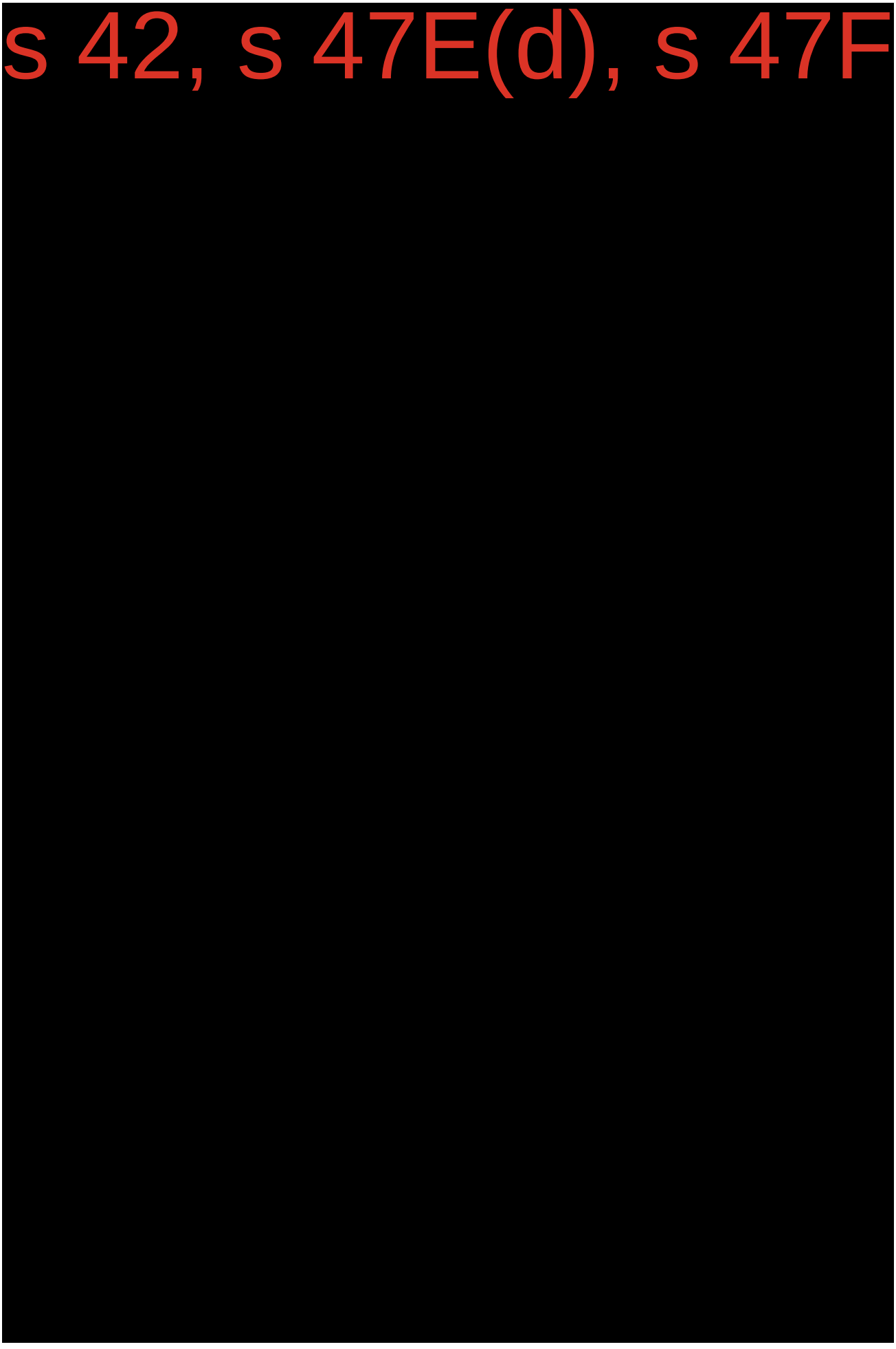
Name	Position	Date

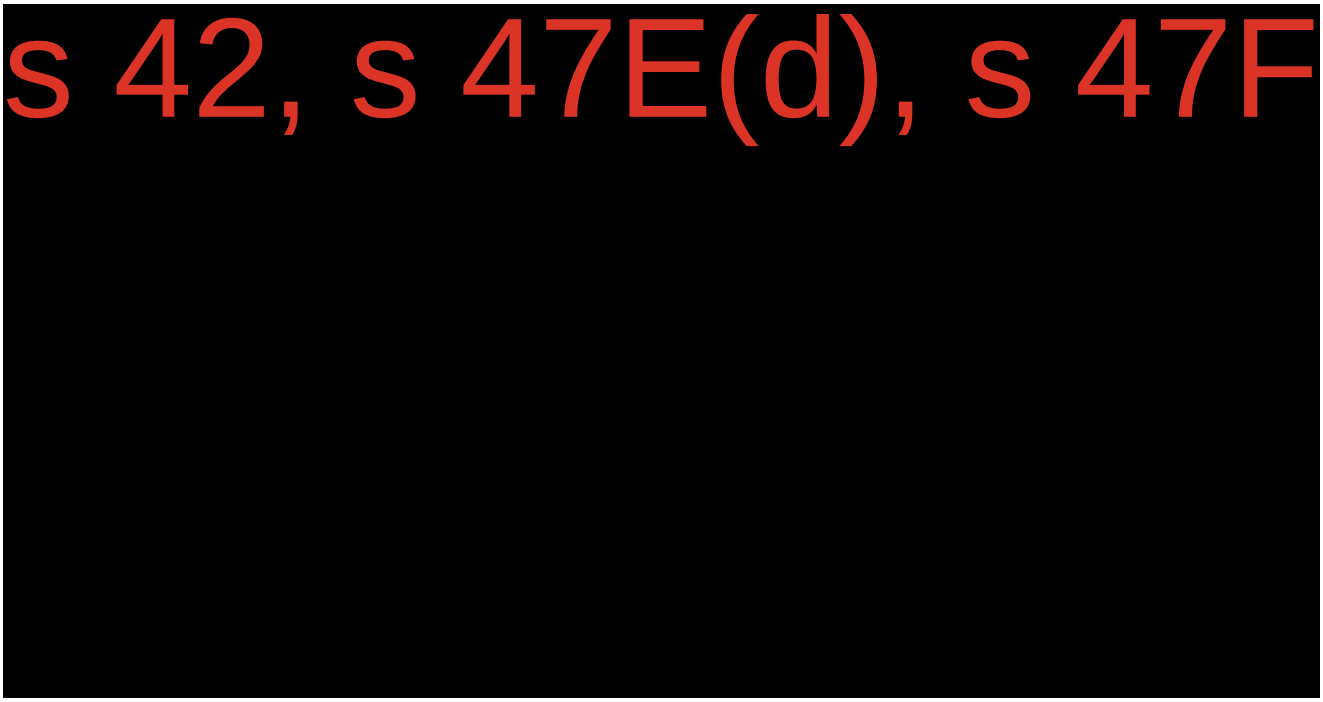
Approver Sign-off

Name	Position	Date

Privacy Officer Sign-off

Name	Date


s 42, s 47E(d), s 47F


s 42, s 47E(d), s 47F

Threshold assessment template

Project Details

Project name	
Date	
Project manager	
Threshold assessment drafter	
Description of the project	*Include a brief description of the project including whether it is a new or existing project. If it is an existing project, describe the proposed changes to the personal information handling practices. You may wish to include links to more detailed project documentation.*
Describe the types of personal information being handled as part of the project	*Brief description of the personal information that will be handled (including personal information that will be collected, used or disclosed, stored, destroyed, de-identified).*
Is there legal authority for the proposed information handling activity?	*Is there legal authority for the proposed information handling activity (for example, is there an existing law that authorises the collection, use or disclosure of personal information for the purposes of the project)? Are there any secrecy provisions that may apply to the proposed information handling activity? Does the information handling activity align with your agency's functions and activities?*
Stakeholders	*List the internal and external stakeholders who have an interest in, or will be affected by, the project. It may be necessary to consult with other areas within your agency, partner agencies or other organisations. You may also approach your agency's Privacy Officer for assistance with completing a threshold assessment or to discuss the project's approach to personal information handling.*

Part 1: Does the project or initiative involve new or changed ways of handling personal information?

☐ Yes — Complete Part 2 of the assessment below.

☐ No — It is not necessary to complete a PIA. Record the decision at Part 3 below and file this assessment with your privacy officer.

Part 2: Determining whether there is the potential for a high privacy risk

Consider the following questions and record each answer as 'yes' or 'no'. The purpose of these questions is to you help you screen for factors which point to the potential for a high privacy risk project. It is important to note that these questions are non-exhaustive, and you should also consider whether there are any other relevant factors that may indicate that your project has the potential to be a high privacy risk project.

Will the project involve:	**Yes**	**No**
Handling large amounts of personal information? *Consider the amount of personal information and the number of individuals that will be impacted by your project. Even if you consider that each individual will only have a small chance of suffering a negative impact, handling personal information on a large scale can increase the privacy risk associated with your project. You should also consider whether your project will result in significant increases in the volume of personal information being handled through new or existing channels.*	☐	☐
Handling sensitive information? *Sensitive information includes, but is not limited to, information about an individual's racial or ethnic origin, political opinions, religious beliefs or affiliations, criminal records, sexual orientation or practices, biometric information[1], health information and genetic information.* *The privacy risk associated with your project can increase if sensitive information is involved given the potential for adverse consequences for an individual, or those associated with the individual, if it is*	☐	☐

[1] Biometric information is an electronic copy of an individual's face, fingerprints, iris, palm, signature or voice.

Will the project involve:	Yes	No
mishandled (for example, discrimination, mistreatment, humiliation or embarrassment).		
Sensitivities based on the context in which the project will operate? *Consider the context and circumstances surrounding the project. Are there prior concerns over this type of handling or activity? Is the project likely to have community support? Is the handling of personal information novel in any way? What is the current state of technology in this area and has there been any previously identified security or technology flaws? Are there any current issues of public concern that you should factor in? What is the nature of your relationship with individuals that may be impacted by the project? How much control will they have over the handling of their personal information? Would they expect you to use their personal information in this way?*	☐	☐
Handling personal information of individuals with particular needs? *Consider whether the activity may have greater sensitivities or disproportionate impacts on certain populations or groups of individuals. This could include children and seniors, people with impaired intellectual or physical functioning, people who are not native speakers of the local language, people with low levels of literacy or education, people from a low socio-economic background, people experiencing financial hardship, people who are Aboriginal or Torres Strait Islanders.* *An individual's circumstances, or the increased power imbalance between the individual and an agency, may mean, for example, they are unable to easily consent to, or oppose, the handling of their personal information, understand its implications, or exercise control over their personal information.*	☐	☐
Handling personal information in a way that could have a significant impact on the individuals concerned? *Consider the potential consequences for the individuals concerned. For example, negative impacts on physical and mental wellbeing, reduced access to public services, discrimination, financial loss or identity theft. Also consider whether the project has a significant collective impact on society, for example, increased surveillance and monitoring activities or the establishment of sensitive personal information sharing arrangements between the Commonwealth and other entities.*	☐	☐

Activity-based risk factors

Will the project involve:	Yes	No
Using or disclosing personal information for secondary purposes? *A 'secondary purpose' is any purpose other than the primary purpose for which the APP entity collected the personal information.*	☐	☐
Disclosing personal information outside of your agency? *Consider whether your project will involve sharing personal information with another agency, organisation or to any individuals other than the individual to whom the information relates. This might include the use of contractors or sub-contractors. Also consider whether your project will require the disclosure of personal information overseas or to an overseas-based company.*	☐	☐
Using or disclosing personal information for profiling or behavioural predictions? *This includes valuation or scoring, profiling and predicting (including in relation to economic situation, health, personal preferences or interests, reliability or behaviour, location or movements).*	☐	☐
Using personal information for automated decision-making? *This might include the use of artificial intelligence technologies or data analytics techniques on personal information to produce insights for policy-making or improved service delivery. It might also include using automated decision-making to make decisions that affect the rights, entitlements and opportunities of an individual.*	☐	☐
Systematic monitoring or tracking of individuals? *For example, the introduction or enhancement of a surveillance system, the monitoring of communications, tracking an individual's geolocation or behaviour.*	☐	☐
Collecting personal information without notification to, or consent of, the individual? *This might include collecting personal information about an individual from a third party without the individual's knowledge or consent. It might also include collecting personal information compulsorily under an existing, or proposed, legislative authority.*	☐	☐

Will the project involve:	Yes	No
Data matching or data linkage? *For example, a new data matching program combining, comparing or matching personal information obtained from multiple sources or a data linkage[2] project where information about the same person from different sources is brought together to create a unified dataset.*	☐	☐
Developing legislation to modify the operation of one or more APPs or which seeks to rely on the required or authorised by law exception to the APPs? *This might include legislation or delegated legislation that seeks to modify the operation of one or more APPs in certain circumstances. It might also include legislation that seeks to rely on the required or authorised an exception to the APPs (such as legislation authorising the use or disclosure of personal information).*	☐	☐

Part 3: Decision & declaration

If you have answered 'Yes' to any of the questions in Part 2, a PIA is likely to be required. If you are uncertain as to whether a PIA is required, you are strongly encouraged to seek support from your agency's privacy officer to ensure your assessment is thorough and complete. If still unsure, err on the side of caution and conduct a PIA.

Based on your answers above, is a PIA required?

☐ Yes Yes, a PIA is required.

☐ No No, a PIA is not required.

[2] Data linkage may also be referred to as 'data integration'.

Outline why it is not necessary to complete a PIA. This may be because the project does not involve personal information (for example, de-identified data is being used) or the project does not involve a new or changed way of handling personal information (refer to your assessment at Part 1 above). If the project is not new, you could include a description of how privacy risks have previously been assessed and are being managed.

If you have ticked one of the boxes in Part 2 above, but have determined that a PIA is not necessary, outline your reasons why. It is the responsibility of each agency to be able to justify why a new or changed way of handling personal information does not have the potential to be high privacy risk.

Assessor Sign-off

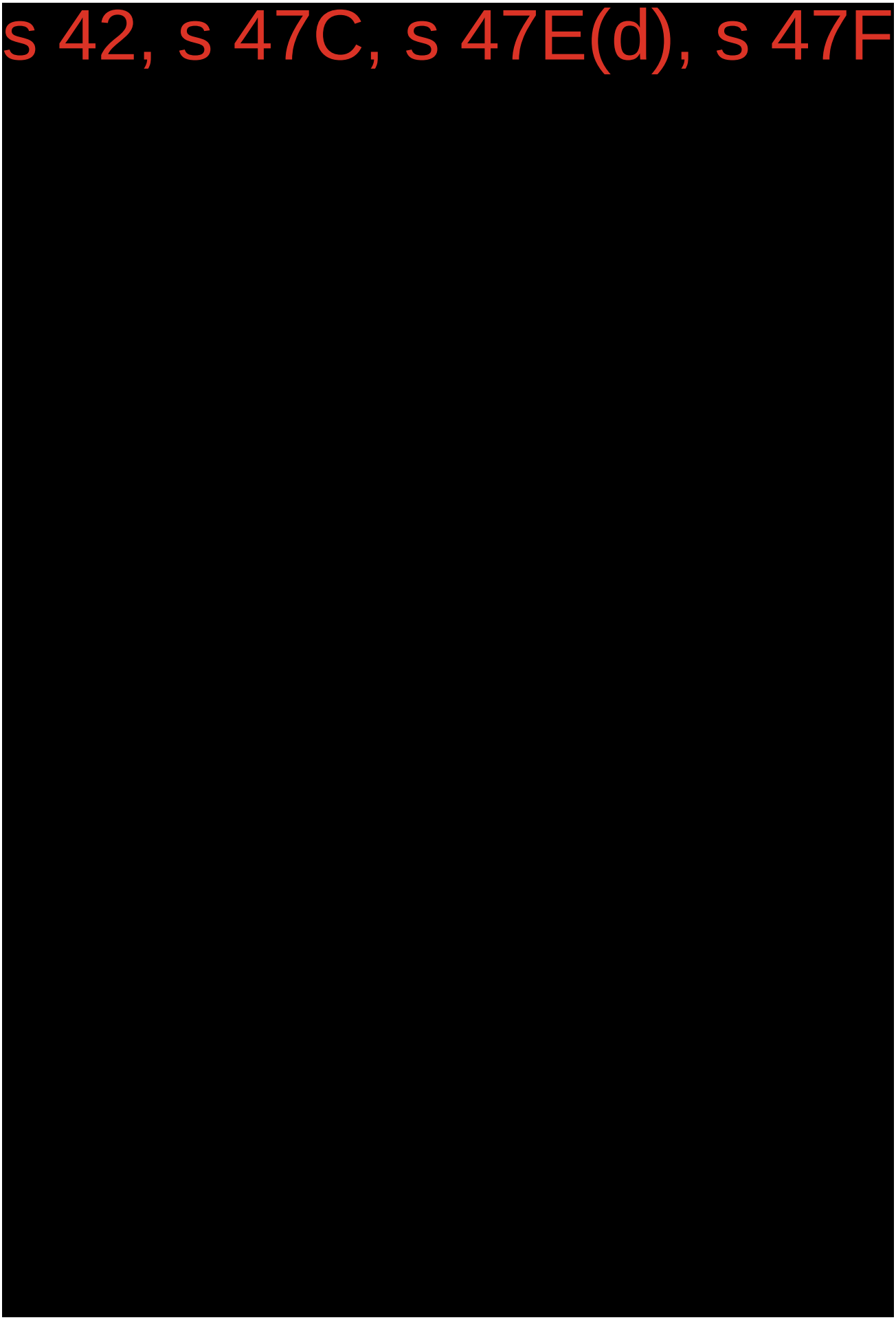
Name	Position	Date

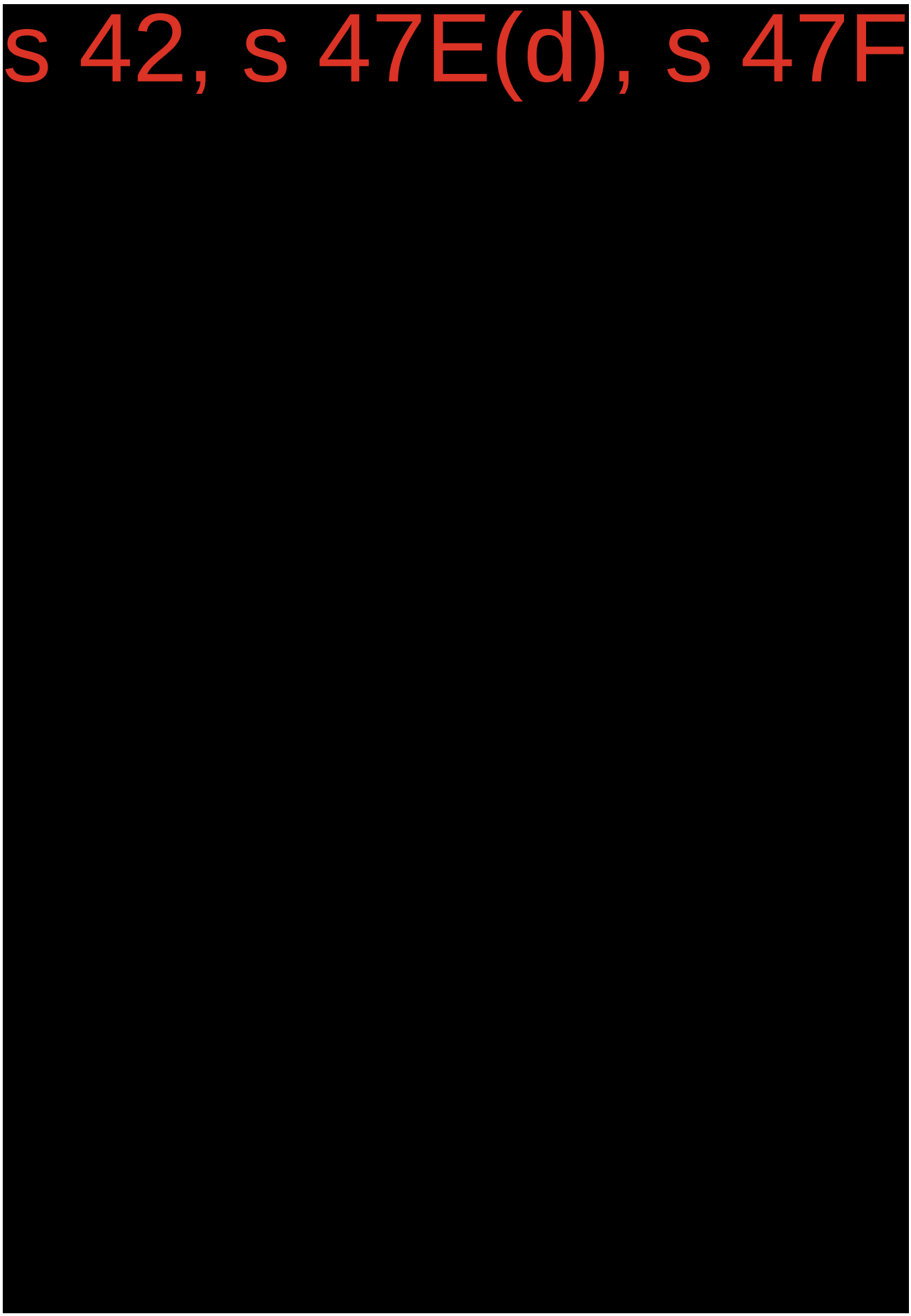
Approver Sign-off

Name	Position	Date

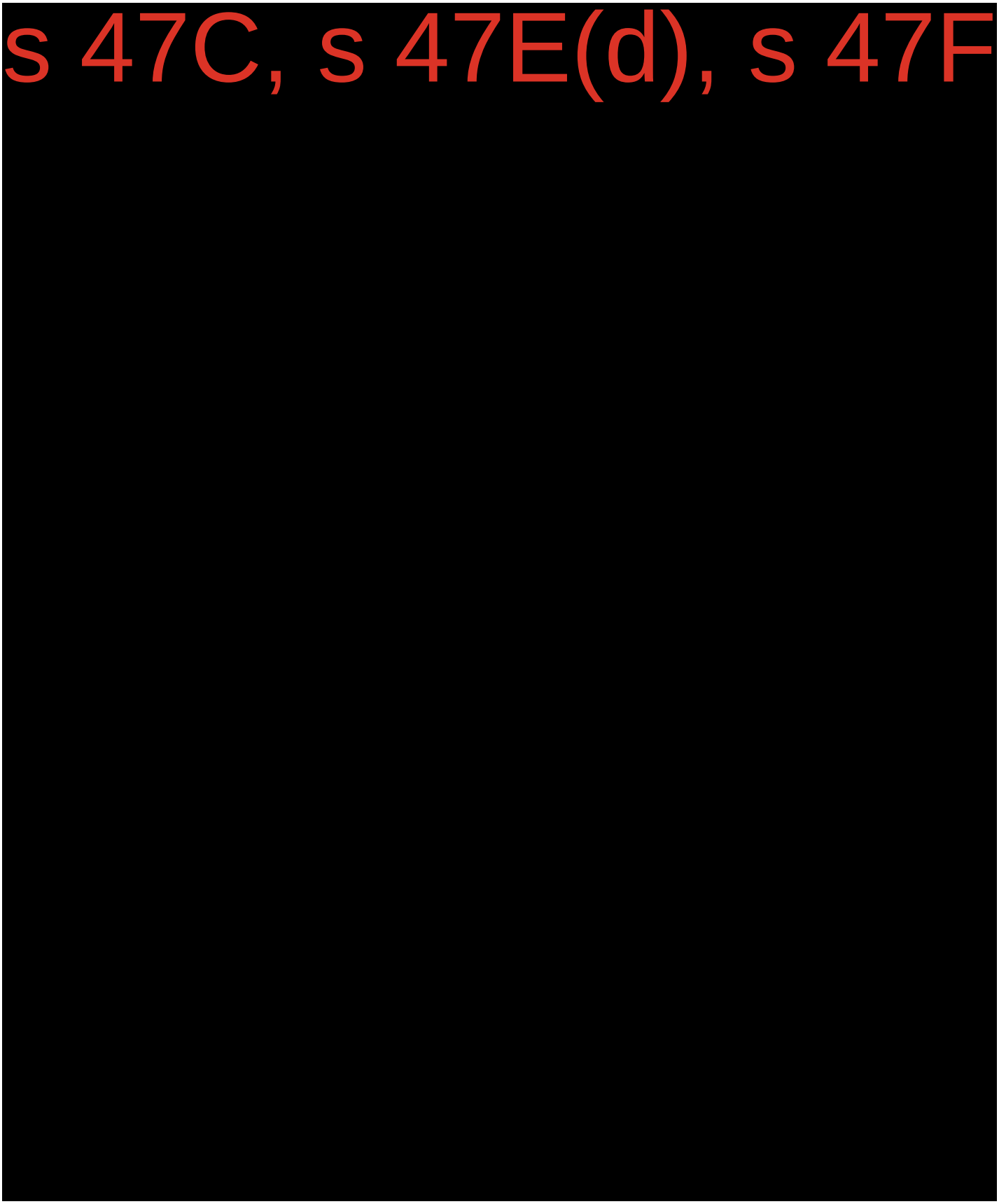
Privacy Officer Sign-off

Name	Date


s 42, s 47C, s 47E(d), s 47F


s 42, s 47E(d), s 47F


s 42, s 47F


s 47C, s 47E(d), s 47F

s 47C, s 47E(d), s 47F

Part 1: Does the project or initiative involve new or changed ways of handling personal information?

☐ Yes — Complete Part 2 of the assessment below.

☑ No — It is not necessary to complete a PIA. Record the decision at Part 3 below and file this assessment with your privacy officer.

Part 2: Determining whether there is the potential for a high privacy risk

Consider the following questions and record each answer as 'yes' or 'no'. The purpose of these questions is to you help you screen for factors which point to the potential for a high privacy risk project. It is important to note that these questions are non-exhaustive, and you should also consider whether there are any other relevant factors that may indicate that your project has the potential to be a high privacy risk project.

Will the project involve:	Yes	No
Handling large amounts of personal information? *Consider the amount of personal information and the number of individuals that will be impacted by your project. Even if you consider that each individual will only have a small chance of suffering a negative impact, handling personal information on a large scale can increase the privacy risk associated with your project. You should also consider whether your project will result in significant increases in the volume of personal information being handled through new or existing channels.*	☐	☑
Handling sensitive information? *Sensitive information includes, but is not limited to, information about an individual's racial or ethnic origin, political opinions,*	☑	☐

Will the project involve:	Yes	No
religious beliefs or affiliations, criminal records, sexual orientation or practices, biometric information[1], health information and genetic information. *The privacy risk associated with your project can increase if sensitive information is involved given the potential for adverse consequences for an individual, or those associated with the individual, if it is mishandled (for example, discrimination, mistreatment, humiliation or embarrassment).*		
Sensitivities based on the context in which the project will operate? *Consider the context and circumstances surrounding the project. Are there prior concerns over this type of handling or activity? Is the project likely to have community support? Is the handling of personal information novel in any way? What is the current state of technology in this area and has there been any previously identified security or technology flaws? Are there any current issues of public concern that you should factor in? What is the nature of your relationship with individuals that may be impacted by the project? How much control will they have over the handling of their personal information? Would they expect you to use their personal information in this way?*	☐	☑
Handling personal information of individuals with particular needs? *Consider whether the activity may have greater sensitivities or disproportionate impacts on certain populations or groups of individuals. This could include children and seniors, people with impaired intellectual or physical functioning, people who are not native speakers of the local language, people with low levels of literacy or education, people from a low socio-economic background, people experiencing financial hardship, people who are Aboriginal or Torres Strait Islanders.* *An individual's circumstances, or the increased power imbalance between the individual and an agency, may mean, for example, they are unable to easily consent to, or oppose, the handling of their personal information, understand its implications, or exercise control over their personal information.*	☑	☐

[1] Biometric information is an electronic copy of an individual's face, fingerprints, iris, palm, signature or voice.

Will the project involve:	Yes	No
Handling personal information in a way that could have a significant impact on the individuals concerned? *Consider the potential consequences for the individuals concerned. For example, negative impacts on physical and mental wellbeing, reduced access to public services, discrimination, financial loss or identity theft. Also consider whether the project has a significant collective impact on society, for example, increased surveillance and monitoring activities or the establishment of sensitive personal information sharing arrangements between the Commonwealth and other entities.*	☐	☑

Activity-based risk factors

Will the project involve:	Yes	No
Using or disclosing personal information for secondary purposes? *A 'secondary purpose' is any purpose other than the primary purpose for which the APP entity collected the personal information.*	☐	☑
Disclosing personal information outside of your agency? *Consider whether your project will involve sharing personal information with another agency, organisation or to any individuals other than the individual to whom the information relates. This might include the use of contractors or sub-contractors. Also consider whether your project will require the disclosure of personal information overseas or to an overseas-based company.*	☐	☑
Using or disclosing personal information for profiling or behavioural predictions? *This includes valuation or scoring, profiling and predicting (including in relation to economic situation, health, personal preferences or interests, reliability or behaviour, location or movements).*	☐	☑
Using personal information for automated decision-making? *This might include the use of artificial intelligence technologies or data analytics techniques on personal information to produce insights for policy-making or improved service delivery. It might also include using automated decision-making to make decisions that affect the rights, entitlements and opportunities of an individual.*	☐	☑

Will the project involve:	Yes	No
Systematic monitoring or tracking of individuals? *For example, the introduction or enhancement of a surveillance system, the monitoring of communications, tracking an individual's geolocation or behaviour.*	☐	☑
Collecting personal information without notification to, or consent of, the individual? *This might include collecting personal information about an individual from a third party without the individual's knowledge or consent. It might also include collecting personal information compulsorily under an existing, or proposed, legislative authority.*	☐	☑
Data matching or data linkage? *For example, a new data matching program combining, comparing or matching personal information obtained from multiple sources or a data linkage[2] project where information about the same person from different sources is brought together to create a unified dataset.*	☐	☑
Developing legislation to modify the operation of one or more APPs or which seeks to rely on the required or authorised by law exception to the APPs? *This might include legislation or delegated legislation that seeks to modify the operation of one or more APPs in certain circumstances. It might also include legislation that seeks to rely on the required or authorised an exception to the APPs (such as legislation authorising the use or disclosure of personal information).*	☐	☑

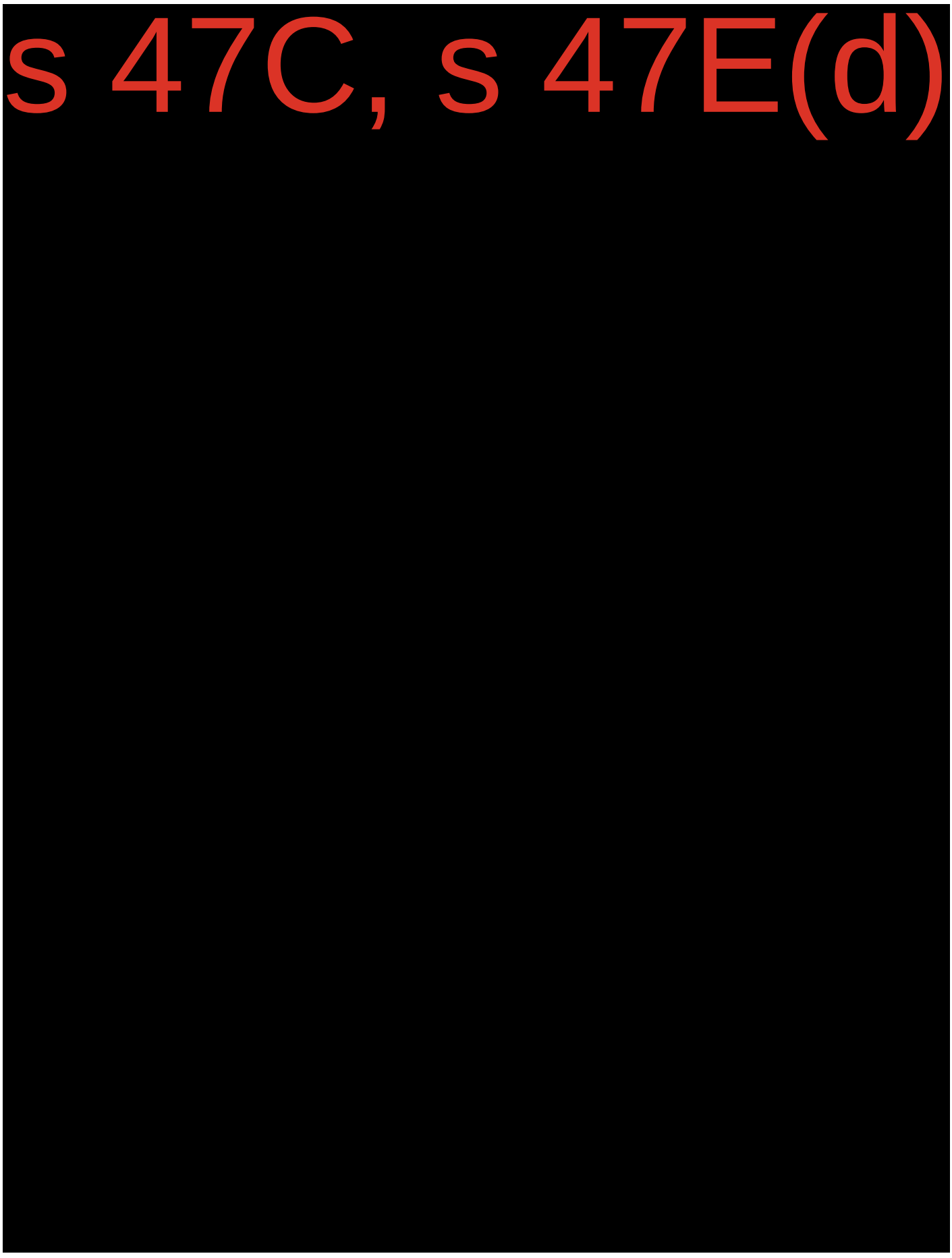
Part 3: Decision & declaration

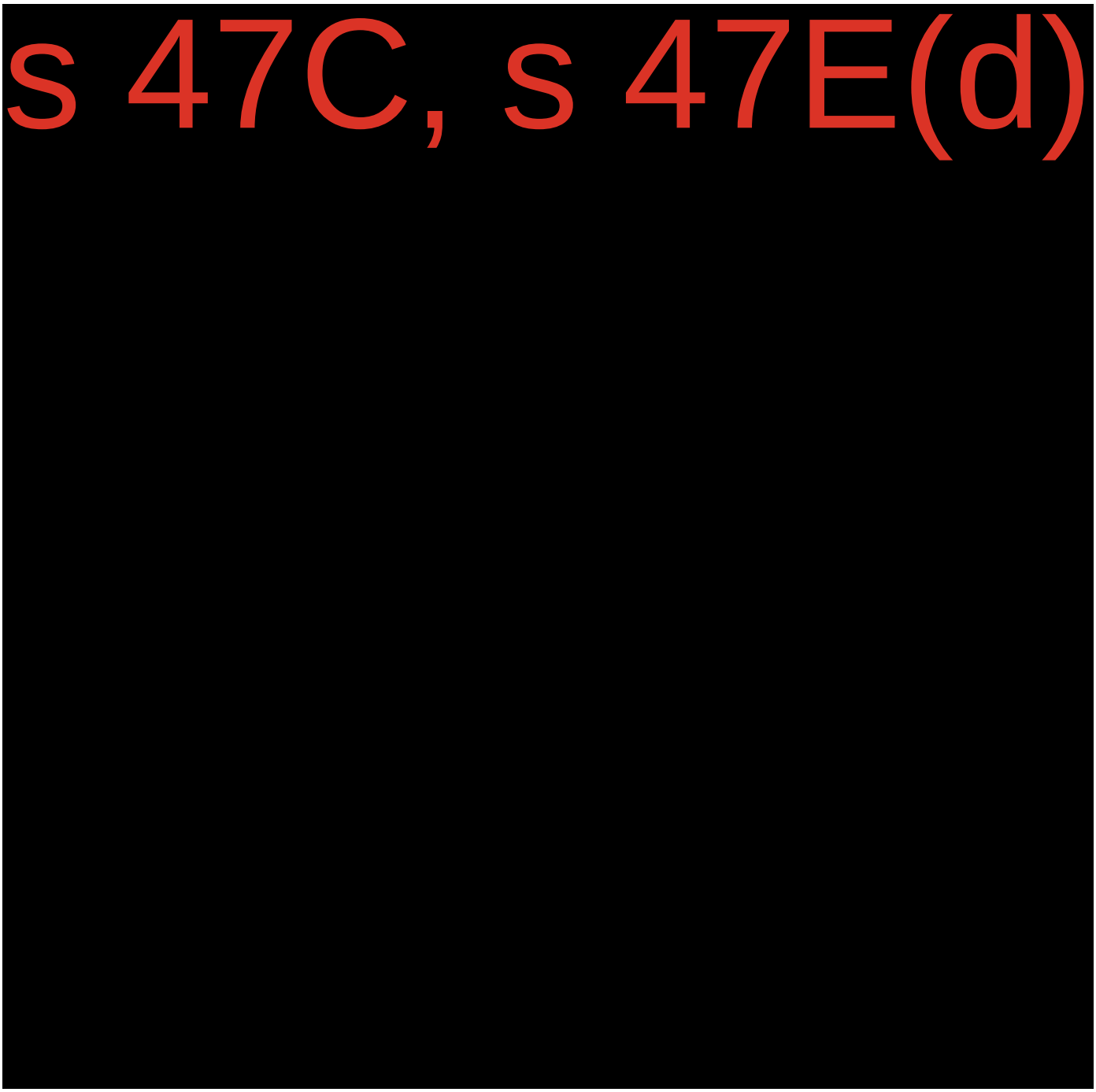
If you have answered 'Yes' to any of the questions in Part 2, a PIA is likely to be required. If you are uncertain as to whether a PIA is required, you are strongly encouraged to seek support from your agency's privacy officer to ensure your assessment is thorough and complete. If still unsure, err on the side of caution and conduct a PIA.

Based on your answers above, is a PIA required?

☐ Yes Yes, a PIA is required.

[2] Data linkage may also be referred to as 'data integration'.


s 47C, s 47E(d)


s 47C, s 47E(d)

Assessor Sign-off

Name	Position	Date

Approver Sign-off

Name	Position	Date

Privacy Officer Sign-off

Name	Date