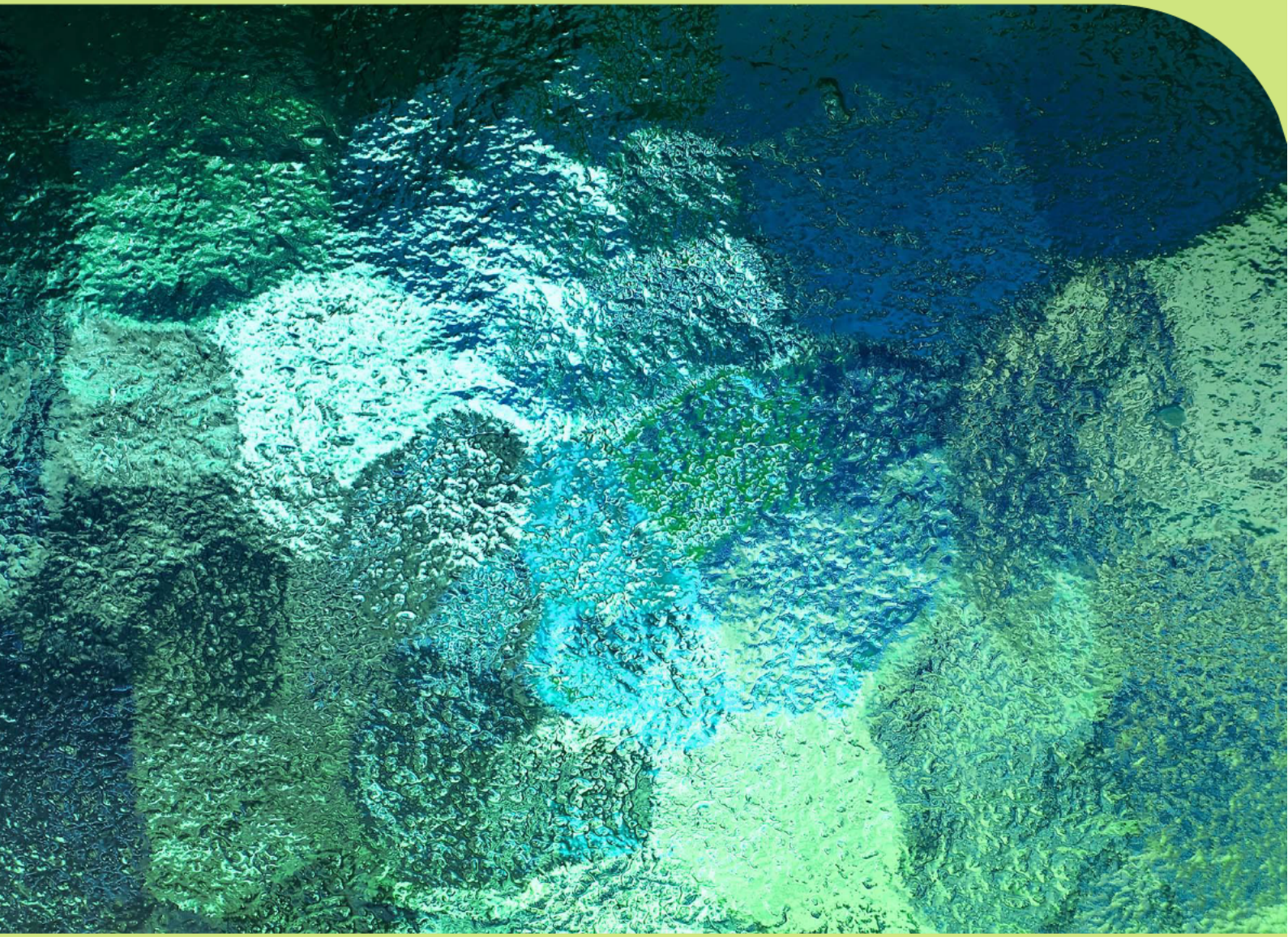
Office of Information Commissioner (OAIC)

Resolve PIA

Privacy Impact Assessment - April 2024



CLAYTON UTZ

CONTENTS

1. Executive summary

The Project: Resolve Enterprise Case Management System

The Resolve Enterprise Case Management System (**Resolve**) is a case management system used by the Office of the Australian Information Commissioner (**OAIC**) in the performance of the Australian Information Commissioner's (**IC**) functions under Australian law (the **Project**).

Resolve allows authorised users, comprising s47E - operations of agencies [redacted] to create a matter in Resolve and to use the functionality of the platform to manage that matter through to resolution, including by storing documents, preparing emails, producing reports, creating tasks and managing workflows.

s47E - operations of agencies [redacted]

Not all OAIC employees have access to Resolve. For those employees who do have access, permissions are applied to ensure that information is accessible on a 'need to know' basis and only to those who have a business need. All users of Resolve must access the system through the DEWR protected network and, except in exceptional circumstances, using OAIC issued laptops.

Information handling by Resolve

The nature of the performance of the IC's functions necessarily requires OAIC to collect substantial amounts of personal information, including sensitive information in order to discharge those functions.

While this is so, the overall privacy risk of Resolve is assessed as low in circumstances where:

- Resolve is used by authorised OAIC employees, DEWR administrators and specified external contractors and consultants on the DEWR protected network and primarily on OAIC issued laptops;
- access to personal information on the Resolve platform is limited to specific users on a need-to-know basis only;
- Resolve users undergo annual information security training and are required to acknowledge DEWR's ICT Terms and Conditions of use of information, including the use of personal and sensitive information, prior to accessing the DEWR protected network;
- external contractors and consultants who have a business need to access Resolve must enter into confidentiality deeds with the OAIC including appropriate non-disclosure obligations prior to accessing Resolve; and
- there is limited proposed data sharing and/or disclosure from Resolve, except as otherwise authorised or required by Australian law.

Privacy impacts and recommendations

This privacy impact assessment (**PIA**) has assessed the Resolve project's compliance with the relevant Australian Privacy Principles (**APPs**), listed at Schedule 1 of the *Privacy Act 1988* (Cth) (**Privacy Act**). This PIA concludes that use of Resolve by OAIC achieves compliance with the OAIC's obligations under the Privacy Act and the APPs.

This PIA makes a number of recommendations to enhance the privacy positivity of the Resolve project. These recommendations are summarised in **Section 2** below.

2. Summary of recommendations

The recommendations made in this privacy impact assessment are set out **below**.

Recommendation 1	s47E - operations of agencies [redacted]
OAIC comments	s47E - operations of agencies [redacted]
Recommendation 2	Ensure that the OAIC's staff training, delivered on a rolling basis, on the obligations set out in the Privacy Act and the APPs encompasses the "need to know" principle.
OAIC comments	Staff training material will be reviewed annually to ensure that obligations in the Privacy Act and the APPs encompass the 'need to know' principle.
Recommendation 3	The OAIC should continue to maintain its existing review processes of user access to the Resolve system, which ensure that only users who have a demonstrated business need continue to have access to the database or matters/categories of information within the database.
OAIC comments	The OAIC currently has an audit process to regularly review user access to Resolve files. Additionally, this process will be used when there is a change to team members or there is a change in business need.
Recommendation 4	s47E - operations of agencies [redacted]

	s47E - operations of agencies [redacted]

OAIC comments	s47E - operations of agencies [redacted]

3. About this PIA

3.1 What is a privacy impact assessment?

A PIA is an examination of a project from a privacy perspective. The primary purposes of a PIA are to:

(a) examine how personal information is collected, used and disclosed as part of a project;

(b) assess the compliance of a project with privacy laws and analyse the impacts of the project on personal privacy; and

(c) identify and recommend options for managing, reducing or removing those impacts.

PIAs are conducted to ensure that privacy issues are fully considered in the design and implementation phase of a project. PIAs help ensure that projects meet privacy requirements in legislation and are also consistent with broader community privacy expectations.

3.2 The approach of this PIA

This PIA has been prepared broadly in accordance with the *Guide to undertaking privacy impact assessments* (the **PIA Guide**), published by OAIC.[1]

The PIA Guide recommends that PIAs be conducted in ten steps, but those steps do not need to be undertaken as separate discrete stages (some of them can be done together). Some of those steps involve deciding whether or not a PIA is necessary (a threshold assessment) and planning.

This PIA was conducted in five key stages, as shown **below**.

Figure 1 — PIA stages

Stage	Description	PIA reference
Stage 1	**Project description** *Broadly describe the project, including the aims and whether any personal information will be handled. This stage involves internal consultation to fully understand the project.*	Section 4
Stage 2	**Mapping personal information flows and privacy framework** *Describe and map the project's personal information flows.*	Section 5

[1] Office of the Australian Information Commissioner, *Guide to undertaking privacy impact assessments* (May 2020).

Stage 3	**Privacy impact analysis** *Identify and analyse the project's privacy impact.*	Section 6
Stage 4	**Privacy Management** *Consider how to manage any privacy impact, particularly options that will improve privacy outcomes.*	Section 7
Stage 5	**Recommendations** *Produce a final PIA report covering the above stages and including recommendations.*	Section 7

3.3 Relevant information

This PIA has been prepared in response to the OAIC's request dated 1 August 2023. In preparing this PIA, the following documents have been considered:

- s47E - operations of agencies [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
- Privacy Threshold Assessment prepared by OAIC dated 28 September 2023;
- information obtained from correspondence between us and OAIC;
- the OAIC's privacy policy accessible at < https://www.oaic.gov.au/about-the-OAIC/our-corporate-information/plans-policies-and-procedures/privacy-policy>; and
- various web forms integrated with Resolve (for example, the SmartForm equivalents currently include the Privacy Complaint Form[2], Notifiable Data Breach Form[3], OAIC General Enquiry[4], FOI Complaint Form[5], FOI Extension of Time Request Form[6], Information Commissioner Review Application Form[7], and Opting in to the Privacy Act Form[8]).

Clayton Utz also engaged in a teleconference with OAIC on 3 August 2023 to better understand the scope and the technical background of the Project.

[2] Accessible at < https://forms.business.gov.au/smartforms/servlet/SmartForm.html?formCode=APC_PC&tmFormVersion>.
[3] Accessible at < https://forms.business.gov.au/smartforms/servlet/SmartForm.html?formCode=OAIC-NDB&tmFormVersion>.
[4] Accessible at < https://forms.business.gov.au/smartforms/servlet/SmartForm.html?formCode=APC_ENQ&tmFormVersion>.
[5] Accessible at <https://forms.business.gov.au/smartforms/servlet/SmartForm.html?formCode=ICCA_1>.
[6] Accessible at <https://forms.business.gov.au/smartforms/servlet/SmartForm.html?formCode=ICRF_1>.
[7] Accessible at <https://forms.business.gov.au/smartforms/servlet/SmartForm.html?formCode=ICR_10>.
[8] Accessible at <https://forms.business.gov.au/smartforms/servlet/SmartForm.html?formCode=privacyactoptin&tmFormVersion>.

3.4 Applicable legislation

This PIA considers whether the Project complies with:

- the APPs, found in Schedule 1 of the *Privacy Act 1988* (**Privacy Act**); and
- the *Privacy (Australian Government Agencies — Governance) APP Code 2017* (the **Privacy Code**) which requires a written PIA to be undertaken in certain circumstances. This PIA satisfies the requirements of the Privacy Code.

3.5 Scope, limitations and assumptions

This PIA assesses the privacy risks associated with the OAIC's use of Resolve as its case management system, including the ingestion, storage, use and disclosure of personal and sensitive information in connection with the Resolve platform.

While we understand that personal information may be disclosed from Resolve to other OAIC controlled data storage software ([redacted] for the purpose of linking that information, this PIA does not assess the privacy risks associated with those other [redacted] We understand that a separate PIA has been completed with respect to the OAIC's use of the [redacted]

4. Project description

This part of the PIA gives a broad outline of Resolve's nature and scope.

4.1 What is the Resolve case management system?

Resolve is used by the OAIC to assist the Australian Information Commissioner (AIC) in the performance of their functions under the Privacy Act and the *Freedom of Information Act 1982* (Cth) (**FOI Act**). Resolve is a Microsoft Windows based case management system used by the OAIC to manage activities and functions such as general enquiries, privacy complaints, and Commissioner-initiated investigation and enforcement activities under the Privacy Act, and investigation and review functions under the FOI Act.

Resolve's functionality provides a centralised database to track client data in relation to the activities and functions performed by the OAIC, such as by logging a case/complaint, allocating tasks, managing deadlines, sending updates and correspondence, managing and storing documents through to resolution, and reporting and analysis.

Resolve is a software program which is only available for use by OAIC users, DEWR administrators, and certain external contractors, and consultants who have a business need to access Resolve in the performance of their employment duties. User access to information within Resolve is provided on a need-to-know basis, and all external contractors and consultants must enter s47E - operations of agencies [redacted]

[redacted]

4.2 Who are the users of Resolve?

There are four categories of Resolve users: s47E - operations of agencies [redacted]

Figure 2 — Categories of User

Category of user	Description
s47E - operations of agencies	• s47E - operations of agencies [redacted] • [redacted]

Category of user	Description
	• Information ingested into Resolve is attached to a case/matter s47E - operations of agencies [redacted]
s47E - operations of agencies	• s47E - operations of agencies [redacted] • s47E - operations of agencies [redacted] • s47E - operations of agencies [redacted]
s47E - operations of agencies	• s47E - operations of agencies [redacted] [redacted]
Public users	• Public users have access to the public facing web-forms only, and do not have access to the internal functionality of Resolve. • The integrated Resolve webforms are used to collect information from complainants (i.e. in relation to a privacy complaint) or notifiers (i.e. in relation to a notifiable data breach). The information collected from 'public users' is automatically ingested into Resolve. • Public users consent to their personal and/or sensitive information being collected and disclosed in the ways described in the OAIC privacy policy. This consent is provided by the public user at the time that they submit the web-form.

4.3 Scope of information collected in Resolve

The AIC has a broad range of functions under the Privacy Act and the FOI Act. The method of collection and ingestion of personal and sensitive information into Resolve is dependent on the particular function being undertaken by the AIC. This is set out in **Figure 3** below.

[9] ICT Services - Privileged Accounts (service-now.com)

Information collected as a result of the functions of the AIC is ingested into Resolve either manually (by a s47E - operations of agencies [redacted]), or automatically (via web forms completed by a public user that are integrated with the Resolve platform).

s47E - operations of agencies [redacted]

Figure 3 — Collection and ingestion of information into Resolve

Function	Collected from	Ingested in Resolve
General enquiries	Directly - from individuals, their representatives	Manually - by uploading or recording in Resolve information obtained by email, phone (through the enquiries line); or Automatically - via an integrated webform
Privacy complaints	Directly - from individuals, or their representatives	Manually - by uploading or recording in Resolve information obtained by email, phone (through the enquiries line); or Automatically - via an integrated webform
FOI functions	Directly - from individuals, or their representatives Indirectly - from entities who hold information subject to the review	Manually - by uploading or recording in Resolve information obtained by email, mail, fax (which is converted to an email), phone (through the enquiries line), or secured file sharing; or Automatically - via an integrated webform
IC investigations	Directly - from individuals or entities, or their representatives Indirectly - as a result of the IC's information gathering powers (e.g. s 44 Privacy Act).	Manually - by uploading or recording in Resolve information obtained by email, mail, fax (which is converted to an email), phone (through the enquiries line), or from documents obtained as a result of the IC's information gathering powers
Data Breach Notifications	Directly - from individuals or entities, or their representatives	Manually - by logging a data breach notification in Resolve including the date the incident was notified, the date the Department became aware, and the number of people affected. Automatically - via the integrated web form.
Data Matching Activities	Indirectly - from entities who propose to undertake data matching activities	Manually - by uploading or recording in Resolve information obtained by email, mail, fax (which is converted to an email), phone (through the enquiries line), or from documents obtained as a result of the IC's functions in respect to Data Matching Activities

Function	Collected from	Ingested in Resolve
		(ss 28A(2)(b) and (d) of the Privacy Act).
Other functions as required by Australian law (e.g. FOI requests)	Directly - from individuals, or their representatives	Manually - by uploading or recording in Resolve information obtained by email or mail.
Corporate functions (e.g. employment matters)	Directly - from individuals, or their representatives	Manually - by uploading or recording in Resolve information obtained verbally, by email, phone, or recorded in documents.

5. Resolve Information Flows

Flow	Description
Collection	Type of information collected • In the performance of the functions outlined at section 4.3 above, personal information is collected by the OAIC and ingested into Resolve, such as full names, dates of birth, telephone numbers, and email addresses. Additional personal information may also be collected through the use of Resolve by the OAIC in the exercise of the IC's functions, such as when processing and managing privacy complaints. • Sensitive information is also collected by the OAIC in the exercise of the IC's functions, such as when processing and managing privacy complaints. Resolve does not include default identifiers capable of distinguishing sensitive information from the other forms of information collected in the Resolve system (including, for example, personal information). • Collection of personal information will generally not involve the de-identification of that personal information. While matters such as privacy and freedom of information complaints can be made anonymously in limited circumstances, this does not occur on a general basis as doing so may impact the OAIC's ability to effectively deal with the complaint. In the exercise of the IC's information gathering powers, it may not be possible to collect personal and sensitive information anonymously. Collection of personal information through Resolve - Types of input Personal information, including sensitive information, will be input into Resolve manually, automatically (through web forms) and through third parties. • Personal and sensitive information collected by phone, email, post or file sharing is manually inputted into Resolve s47E - operations of agencies [redacted] • s47E - operations of agencies [redacted] Public users submitting any information to the OAIC using a web form are required to consent to the collection, use and disclosure of their personal information contained in the web form for the purposes of the OAIC addressing their complaint or enquiry. • Information stored on Resolve may also be collected from third parties in the exercise of the IC's functions under the Privacy Act and FOI Act. Where information is collected from third parties in this way, it will be input into Resolve s47E - operations of agencies [redacted]

Flow	Description
Storage	• s47E - operations of agencies [redacted] • [redacted] • [redacted] • Documents produced by Resolve as part of the management of a case (including e-mails) are stored in a central repository that is accessible to only those users who are authorised to access the documents relating to that case. The central repository can be Resolve's file system or a third-party electronic document and records management system (s47E - operations of agencies [redacted] • Although there is the ability for data entered into Resolve to be physically deleted, there may be certain case management procedures and controls external to Resolve which may affect complete deletion, including the operation of the *Archives Act 1983* (Cth). Resolve also allows for data (including personal information) held in the system to be marked as either de-registered (to indicate the data is incorrect) or obsolete (to indicate that it was once correct but is no longer applicable).
Use	• Data, including personal and sensitive information, is used for the performance of the IC's functions pursuant to Australian law only, and not for any other purpose. • Users are allocated permissions based on their user group including what units of data, screens or reports are accessible and what that user can alter. s47E - operations of agencies [redacted] • Users are able to use Resolve to run pre-defined reports and / or develop ad-hoc reports for external reporting purposes. Any data used for external reporting purposes is de-identified and aggregated.

Flow	Description
Disclosure	• s47E - operations of agencies [redacted] • [redacted] • The OAIC will only disclose personal or sensitive information held on Resolve where it is authorised or required by Australian law to do so. Personal and sensitive information may be disclosed for a secondary purpose in the performance of the IC's functions, such as when the OAIC undertakes its compliance and investigatory functions under the Privacy Act. • Personal and sensitive information may also be disclosed to other Commonwealth entities when undertaking data matching and data sharing activities or disclosing information. • Any disclosures of personal information, including sensitive information, will occur by way of a s47E - operations of agencies Resolve to extract any relevant information stored on Resolve to give effect to the required disclosure. That disclosure will then occur manually (for example, by way of the s47E - operations of agencies the relevant and authorised information by way of email).

6. Compliance

6.1 Compliance with privacy obligations under the Privacy Act

The Australian Privacy Principles

The Privacy Act provides that an "*APP entity*" must not do an act, or engage in a practice, that breaches an APP.[10] As an "*agency*", OAIC is an APP entity and is therefore bound by the Privacy Act.[11]

The APPs are set out in Schedule 1 to the Privacy Act. The APPs regulate, among other things, the collection, use and disclosure of "*personal information*" and "*sensitive information*" by APP entities. This PIA analyses Resolve against the APPs, having regard to the guidance set out in the APP Guidelines.[12] The APP Guidelines outline the mandatory requirements of the APPs, how the OAIC interprets the APPs, matters the OAIC may take into account when exercising functions and powers under the Privacy Act, and good privacy practice to supplement compliance with the mandatory requirements in the APPs.[13]

Section 95B

Section 95B of the Privacy Act prescribes particular requirements for agencies entering into Commonwealth contracts to ensure that a contracted Commonwealth service provider must take contractual steps to maintain compliance with the Privacy Act for acts or practices engaged in pursuant to the contract. The purpose of this provision is to ensure that entities with whom the Commonwealth has contracted do not engage in conduct that would constitute a breach of the Commonwealth's privacy obligations (if that conduct were to be carried out by the Commonwealth).

Notifiable Data Breach Scheme

The Notifiable Data Breach Scheme relevantly requires the OAIC to notify affected individuals and the Office of the Australian Information Commissioner when a data breach is likely to result in serious harm to an individual whose personal information is involved in that data breach.

A data breach will occur where personal information held by the OAIC is subject to unauthorised access or disclosure, or loss. This could include (but is not limited to) a database where personal information is being stored being hacked, a particular device holding personal information being hacked, lost or stolen, or personal information being inadvertently disclosed to an unauthorised recipient.

[10] See s 15 of the Privacy Act.
[11] See s 6 of the Privacy Act.
[12] Office of the Australian Information Commission *Australian Privacy Principles Guidelines* (**APP Guidelines**).
[13] See the Preface to the APP Guidelines.

6.2 Compliance assessment table

We have considered compliance against each of the privacy obligations under the Privacy Act in the table below. We have not included analysis in relation to APP 7 which applies only to organisations.[14]

Figure 4 — Privacy compliance assessment table

No.	Privacy Principle	Compliance
APP 1	**Open and transparent management of personal information**	*APP 1 requires that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.* **Satisfied** The Project takes reasonable steps to comply with the APPs and the OAIC privacy policy, including by ensuring that access to personal information stored on Resolve is managed by user access permissions and by using and disclosing information it collects transparently in the ways described in the OAIC's privacy policy.
APP 2	**Anonymity and pseudonymity**	*Where relevant, APP 2 requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.* **Satisfied** Pursuant to APP 2.2(b), it would be impracticable for the Project to engage with individuals anonymously or pseudonymously for the purposes of addressing, managing, or responding to a s47E - operations of agencies [redacted]
APP 3	**Collection of solicited personal information**	*APP entities must not collect solicited personal information other than as prescribed by APP 3. To comply with APP 3, OAIC can only collect personal information that is reasonably necessary for, or directly related to, one or more of its functions or activities. APP entities must only solicit and collect personal information by lawful and fair means, and directly from the individual, unless an exception applies. Sensitive information can only be collected with the consent of the individual unless an exception applies.* **Satisfied**

[14] "Organisation" is defined in s 6C of the Privacy Act and excludes an "agency" (as defined in s 6 of the Privacy Act).

No.	Privacy Principle	Compliance
		Based on the information provided, we are satisfied that the OAIC is collecting personal and sensitive information in a manner that achieves compliance with APP 3. The collection of the personal and sensitive information, as described in the information flows, is directly related to the OAIC's functions. s47E - operations of agencies [redacted]
APP 4	**Dealing with unsolicited personal information**	*APP 4 outlines how APP entities must deal with unsolicited personal information.* **Satisfied with recommendation** We understand that it is possible that the OAIC could collect unsolicited personal information as part of the Project. The OAIC may use or disclose unsolicited personal information collected as part of the Project if the OAIC determines, within a reasonable time, that the unsolicited personal information could have otherwise been collected by the OAIC under APP 3. For example, unsolicited personal information may be provided by a complainant when notifying the OAIC of a privacy complaint through submission of the relevant Resolve webform. However, this information may be able to be collected by the OAIC and used or disclosed in compliance with the APPs where it is reasonably necessary for, or directly related to, one or more of the OAIC's functions or activities which relevantly, may include investigating notifiable data breaches. As such, this APP 4 obligation is satisfied provided that the OAIC: • ensures that there is a management process in place to promptly deal with the receipt of any unsolicited personal information; and • where the OAIC does receive unsolicited personal information, which it could not have collected under APP 3, the OAIC should ensure that such information is either destroyed or de-identified as soon as practicable - provided the information is not contained in a 'Commonwealth record' (section 3 of the *Archives Act 1983* (Cth)).

No.	Privacy Principle	Compliance
APP 5	**Notification of the collection of personal information**	*APP 5 outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters. This includes the purposes for which the personal information is collected.*
		Satisfied with recommendation We are satisfied that the requirements set out under APP 5 have been met in relation to the Project, provided that the recommendation set out in section 7.2 below is implemented. Individuals who provide the OAIC with their personal information (which is then collected in the Resolve system) will be informed of the matters set out in APP 5 through the OAIC privacy policy. Individuals acknowledge the terms of the OAIC privacy policy at the time of submitting a Resolve web form. We are satisfied that the OAIC privacy policy addresses the matters necessary to achieve compliance with APP 5.
APP 6	**Use or disclosure of personal information**	*APP 6 outlines the circumstances in which an APP entity may use or disclose personal information that it holds.*
		Satisfied The personal information collected in the Project will be used and / or disclosed for the primary purpose, or otherwise in accordance with APP 6. In particular, as set out in the OAIC's privacy policy, personal information collected as part of the Project will be used or disclosed by the OAIC in the exercise of its powers or performance of its functions and duties under Australian law, including for example, to carry out privacy and freedom of information investigations.
APP 8	**Cross-border disclosure**	*APP 8 requires APP entities to take steps to protect personal information before it is disclosed overseas.*
		Satisfied Based on the information provided, the Resolve systems will not be used to disclose personal information overseas. All personal information handled by the OAIC as part of the Project will be s47E - operations of agencies [redacted] Where personal information stored on Resolve is disclosed overseas as part of the OAIC's broader functions and activities, this must be done in compliance with APP 8 and the OAIC's privacy policy.
APP 9	**Adoption, use or disclosure of government related identifiers**	*APP 9 restricts the adoption, use or disclosure of certain government related identifiers (like Medicare/Centrelink numbers, drivers licenses or passport numbers) by organisations. It does not apply to agencies.*
		Not applicable APP 9 does not apply to agencies.

No.	Privacy Principle	Compliance
APP 10	**Quality of personal information**	*APP 10 requires APP entities to take reasonable steps to protect personal information they collect is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.* **Satisfied** The OAIC has an ongoing obligation to ensure the personal information it collects and stores is accurate, up-to-date, complete and relevant. Based on the information provided, the Project will be conducted in compliance with the OAIC privacy policy, which includes mechanisms for updating and auditing personal information held by the OAIC from time to time on an ad-hoc basis. The Resolve system also includes the functionality for the personal information of users to be updated.
APP 11	**Security of personal information**	*APP 11 requires APP entities to take reasonable steps to protect personal information held by them from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.* **Satisfied** Based on the information provided, we consider that compliance with APP 11 is satisfied. s47E - operations of agencies [redacted]
APP 12 **APP 13**	**Access to and correction of personal information**	*APP 12 and APP 13 set out APP entities' privacy obligations when an individual requests access to, or correction or, their personal information.* **Satisfied** Based on the information provided, the Project will be conducted in compliance with the OAIC privacy policy, which includes mechanisms for accessing and correcting personal information held by the OAIC. The Resolve system also includes the functionality for the personal information of users to be corrected.

Privacy Principle	Compliance
S 95B ***Privacy Act***	*Under section 95B of the Privacy Act, an agency entering into a Commonwealth contract must take contractual measures to ensure that a contracted service provider for the contract does not do an act, or engage in a practice, that would breach an APP if done or engaged in by the agency. The agency must ensure that the Commonwealth contract does not authorise a contracted service provider, nor a subcontractor, to do or engage in such an act or practice.*
	Satisfied On the basis that all personal information for the Project will be handled by the OAIC and no external stakeholders will be contracted to deliver the Resolve system, the obligations in s 95 are not engaged in relation to the Project.
Notifiable Data Breach Scheme	*OAIC has obligations under the Notifiable Data Breach (**NDB**) Scheme to notify affected individuals and the Office of the Australian Information Commissioner (OAIC) when a data breach is likely to result in serious harm to an individual whose personal information is involved. A data breach occurs when personal information an organisation or agency holds is lost or subject to unauthorised access or disclosure.*
	Satisfied On the basis that all personal information for the Project will be handled by the OAIC and no external stakeholders will be contracted to deliver the Resolve system, OAIC is responsible for the obligations in relation to the NDB scheme.

7. Consideration of specific privacy issues

7.1 Management of unsolicited personal information

Further to our analysis in section 0 above and given the investigatory and compliance functions of the OAIC, we understand that it is anticipated that the Resolve system may collect some unsolicited personal information. In particular, unsolicited personal information may be collected through the open-ended inputs included as part of the Resolve web forms, via third parties or through direct disclosure to OAIC employees via email or telephone. It is anticipated that this unsolicited personal information may then, where compliant with APP 4, be used by the OAIC in pursuant to its functions or activities under Australian law.

In accordance with APP 4, unsolicited personal information may only be used or disclosed by the OAIC where the OAIC determines, within a reasonable time, that the unsolicited personal information could have otherwise been collected by the OAIC under APP 3. This means that, in order to be used or disclosed, the unsolicited personal information must be reasonably necessary for, or directly related to, one or more of the OAIC's functions or activities.

To comply with APP 4, the OAIC should consider developing processes and policies in place to ensure that:

- unsolicited personal information collected either manually or automatically (through the Resolve web forms) is identified and assessed by OAIC employees (in accordance with the requirements below) within a reasonable period of time;
- OAIC employees are comfortable, and have the appropriate tools, to assess whether the unsolicited personal information falls within the scope of APP 3 in that the information is reasonably necessary for, or directly related to, one or more of the OAIC's functions or activities, such that the OAIC could have collected the information itself; and
- where personal information which could not have been collected under APP 3 is received by the OAIC, that information is either destroyed or de-identified as soon as practicable, provided the information is not contained in a 'Commonwealth record' (section 3 of the *Archives Act 1983* (Cth)).

The OAIC may consider developing training on how to effectively deal with unsolicited information, such as the development of a module addressing the collection, management and de-identification or destruction of unsolicited personal information to be included as part of the annual information handling training (see section 7.2 below).

Recommendation 1	s47E - operations of agencies [redacted]

7.2 Staff training on privacy obligations and "need to know" access to personal and sensitive information

The terms of APP 3 and APP 5 require 'customer facing' OAIC employees to be familiar with the OAIC's obligations set out in the Privacy Act and the APPs.

This is particularly so for OAIC employees who may handle personal or sensitive information as a result of receiving complaints by phone or email. This is because, unlike the Resolve web forms, a complainant submitting a complaint or enquiry over phone or email will not be automatically directed to the OAIC's privacy statement rather, it is the OAIC employee who must ensure the matters set out in the OAIC privacy policy are brought to the complainant's attention.

Under APP 3, the OAIC can only collect personal information that is reasonably necessary for, or directly related to, one or more of its functions or activities. The OAIC must only solicit and collect personal information by lawful and fair means, and directly from the individual, unless an exception applies. Sensitive information can only be collected with the consent of the individual, unless an exception applies.

Further, APP 5 outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters. This includes the purposes for which the personal information is collected.

To comply with APP 3 and APP 5, the OAIC employees who engage with complainants or customers through phone or email must be comfortable, and have the appropriate tools to:

- inform complainants or other customers how their personal information will be used and disclosed;
- obtain consent from complainants when collecting sensitive information and to appropriately record that consent;
- direct complainants or other customers to the OAIC privacy policy and to answer questions in respect to it; and
- uniformly record personal and sensitive information to ensure it is accurate, up to date, and accurate in accordance with APP 10.

The Resolve system will hold personal and sensitive information collected for the purpose of the OAIC performing its functions and activities conferred under Australian law, including for the purpose of undertaking its investigatory and compliance functions. All users of the Resolve system must hold a security clearance and comply with general information handling, privacy, and terms of use policies applicable to the OAIC's information technology systems. Further, only privileged users (of which, there are approximately 1 - 10) are able to grant or change a user's permissions.

s47E - operations of agencies [redacted]

- [redacted]
- [redacted]

- s47E - operations of agencies [redacted]

[redacted]

[redacted]

Recommendation 2	The OAIC's staff training, undertaken on a rolling basis, on the obligations set out in the Privacy Act and the APPs, and as reflected in the APP privacy policy, should encompass the "need to know" principle.

7.3 Regular review of access to Resolve

Further to the discussion at section 0 above, we consider that OAIC should take steps to ensure that user access to the Resolve system is reviewed at regular intervals to ensure only users with a current business need continue to have access to the database.

We understand that OAIC presently undertakes regular and ongoing internal reviews in relation to access which is informed by information about staff movements, including intra-office movements.

Recommendation 3	The OAIC should continue to maintain its existing review processes of user access to the Resolve system, which ensure that only users who have a demonstrated business need continue to have access to the database or matters / categories of information within the database.

7.4 Destruction of personal information

We note that in addition to providing for security of personal information, APP 11 also promotes the destruction and / or de-identification of personal information where the retention of that information is no longer necessary.

Resolve does have the functionality for information held within the system to be deleted, de-registered (to indicate the data is incorrect) or marked obsolete (to indicate that it was once correct but is no longer applicable). However, due to the broad range of functions or activities pursuant to which the OAIC collects and uses personal information, the period of time for which it is appropriate for that information to be held (on the basis it continues to be necessary) may differ.

In this respect, we understand that the OAIC will handle personal information in connection with the Project in the manner provided for in its privacy policy, which also incorporates the OAIC's obligations under the *Archives Act 1983* (Cth).

In order to enhance the privacy positivity of the Project, the OAIC could give consideration to confirming as part of the Project when personal information collected from individuals through the Resolve system can be de-identified or destroyed. We note that policies in this regard should be developed in conjunction with the OAIC's other record-keeping obligations, including

under the *Archives Act 1983* (Cth). In this respect, we understand that the OAIC is currently in the process of updating its Records Authority which is a pre-requisite to the development of any subsequent OAIC policy in relation to the deletion of personal information collected through the Resolve system.

Recommendation 4	s47E - operations of agencies [redacted]

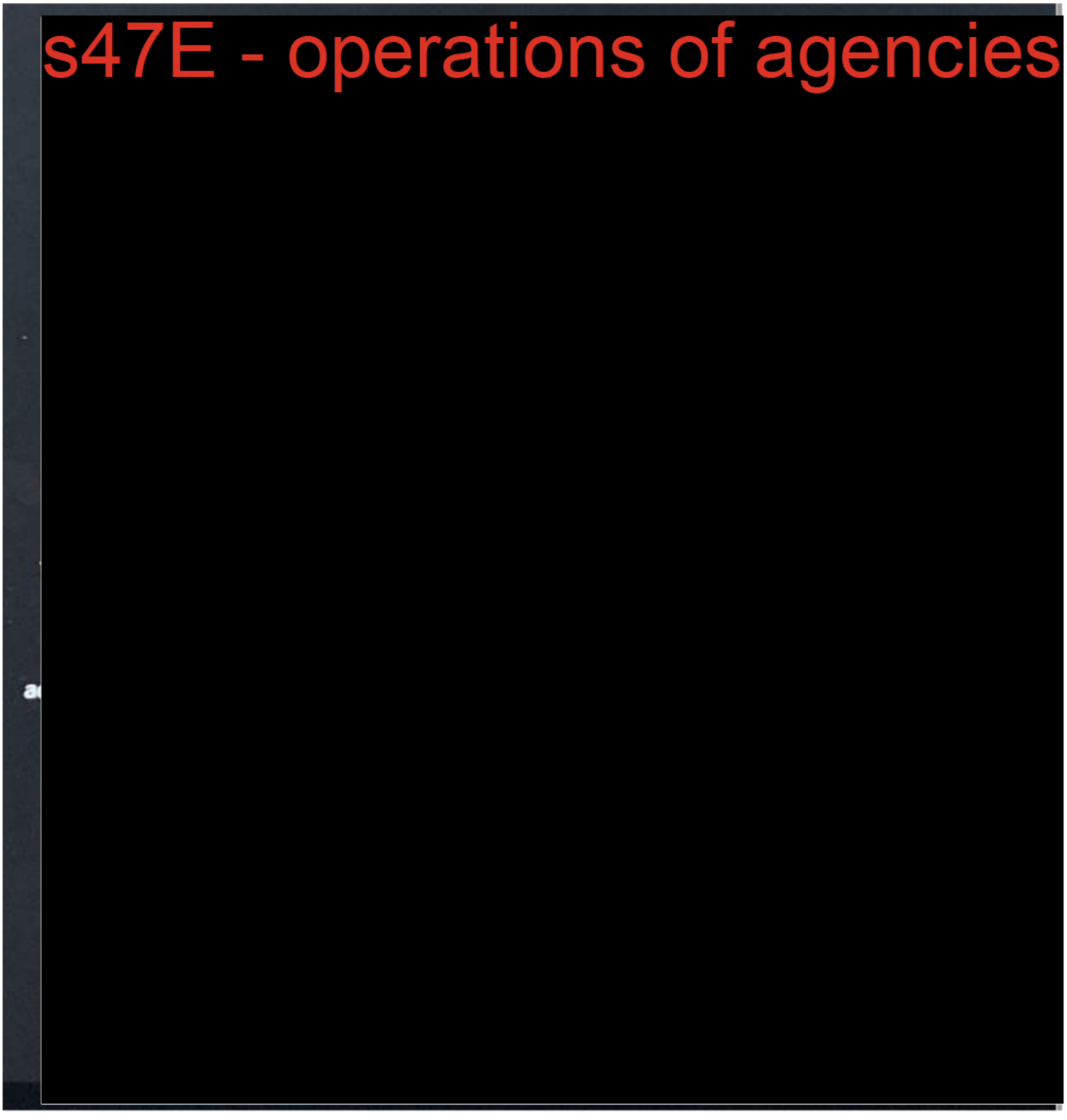
8. Glossary

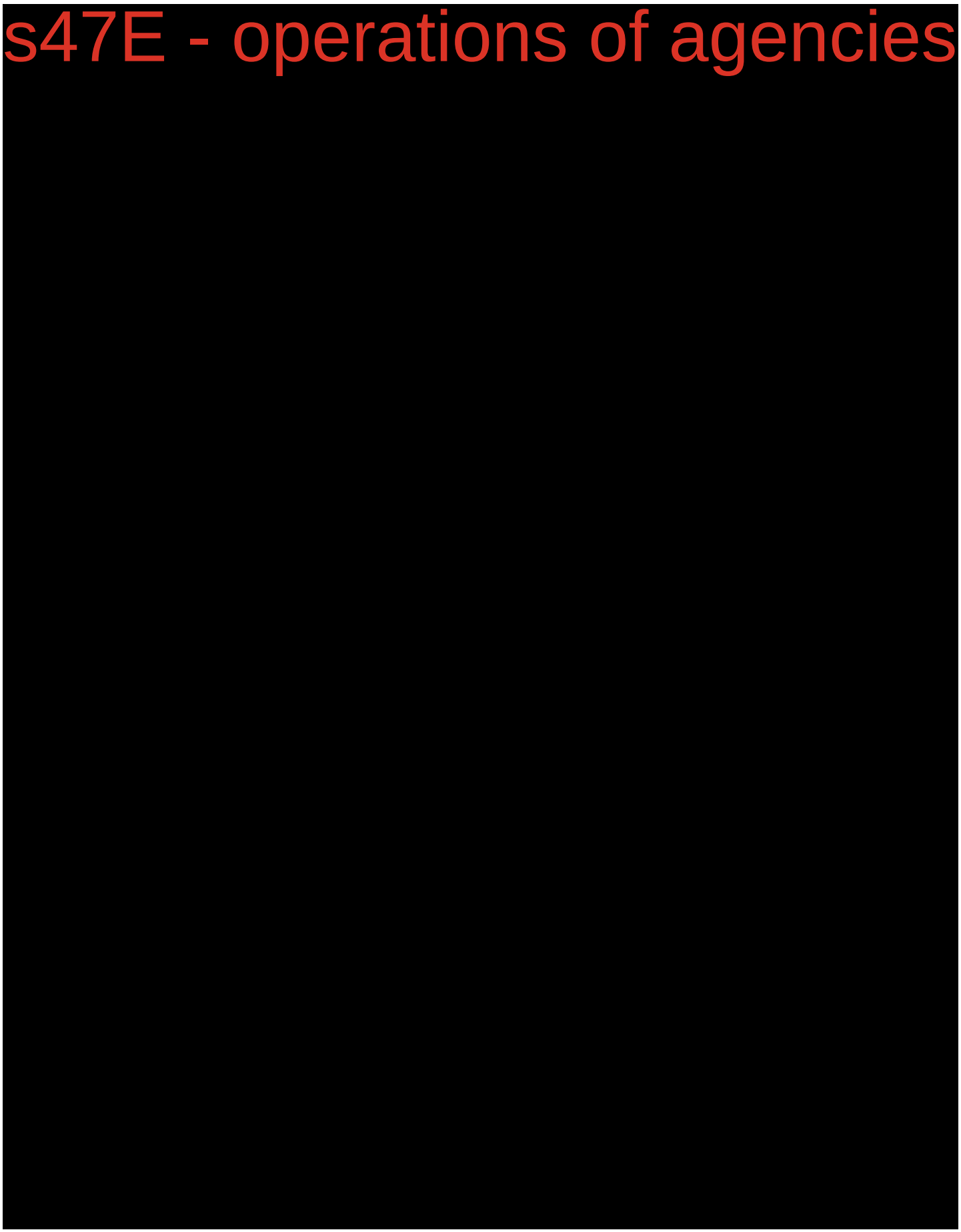
Term/Acronym	Definition
APPs	Australian Privacy Principles, which appear at Schedule 1 of the *Privacy Act 1988* (Cth).
DEWR	Department of Employment and Workplace Relations
FOI Act	*Freedom of Information Act 1982* (Cth)
IC	Information Commissioner
ICT	Information, Communications and Technology
NDB	Notifiable Data Breach
OAIC	Office of Information Commissioner
Personal information	The handling of "personal information" (including "sensitive information") by Australian Commonwealth Government agencies is regulated by the Privacy Act. The term "personal information" is a key concept in the Privacy Act. Whether or not particular information is "personal information" is a threshold question which determines whether the APPs will apply to the handling of the information (and whether we must consider whether the handling of information must be assessed for compliance against the APPs). Personal information is defined in section 6 of the Privacy Act as "*information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not*".
PIA	Privacy Impact Assessment.
PIA Guide	*Guide to undertaking privacy impact assessments*, published by the Office of the Australian Information Commissioner.
Privacy Act	*Privacy Act 1988* (Cth).
Sensitive information	Most "sensitive information" is a special subset of "personal information". The APPs generally afford a higher protection to "sensitive information" in recognition of the fact that there can be adverse consequences for an individual if their sensitive information is mishandled.[15] The term "*sensitive information*" is defined in s 6 of the Privacy Act. It relevantly includes "*health information*" about an individual. The term "*health information*" is defined in s 6FA of the Privacy Act. It relevantly includes:

[15] See paragraph [B.141] of the APP Guidelines.

Term/Acronym	Definition
	(a) information or an opinion about: (i) the health, including an illness, disability or injury, (at any time) of an individual; or (ii) an individual's expressed wises about the future provision of health services to the individual; or (iii) a health service provided, or to be provided, to an individual; (b) other personal information collected to provide or in providing, a health service to an individual; and (c) genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.

Annexure A Privacy Notice




s47E - operations of agencies


s47E - operations of agencies