COMMONWEALTH OMBUDSMAN

Privacy Impact Assessment – Integrated Voice Response (IVR) Implementation

16 March 2023

Report title	Privacy Impact Assessment – Integrated Voice Response (IVR) Implementation
Originating area	Business Intelligence, Improvement and Performance
Date produced	16 March 2023
Cleared by	Director, Business Intelligence, Improvement and Performance Chief Information Officer Privacy Officer, Legal Team
Endorsed by	Chief Operating Officer
Objective file/document	A2319053

Contents

Executive summary **4**

PIA methodology **4**

Project Overview **5**

Personal Information Flows **6**

Privacy Impact Analysis **11**

Compliance check **12**

APP 1 — Open and transparent management of personal information 12

APP 2 — Anonymity and pseudonymity 16

APP 3 — Collection of solicited personal information 17

APP 4 — Dealing with unsolicited personal information 23

APP 5 — Notification of the collection of personal information 23

APP 6 — Use or disclosure of personal information 25

APP 8 — Cross-border disclosure of personal information 26

APP 10 — Quality of personal information 28

APP 11 — Security of personal information 29

APP 12 — Access to personal information 38

APP 13 — Correction of personal information 39

Other considerations 43

Privacy Management – Addressing Risks **45**

QPC User Access Management Standard – Information Security Management Sys **45**

QPC is partner – 'Authorised Organisation' of the Platform Provider (see.... Error! Bookmark not defined.

QPC User Access Management Standard – Information Security Management System ..... Error! Bookmark not defined.

Recommendations **47**

Executive summary

The purpose of this Privacy Impact Assessment (PIA) is to ensure that the information disclosed and collected and stored in undertaking our telephony interactions with complainants/individuals contacting the Office, is managed in line with the Australian Privacy Principles as contained in the *Privacy Act 1988* (Privacy Act).

This PIA was prepared at the request of the Office's Chief Operating Officer. The Office of the Australian Information Commissioner (OAIC) also has powers and functions to direct the provision of a PIA if a proposed activity could have a significant impact on the privacy of individuals: *Privacy Act 1988* (Cth) s 33D. A PIA is required for 'high risk privacy projects' that are likely to have 'a significant impact on the privacy of individuals:' Privacy (Aust Govt Agencies) APP Code 2017 r 12.

The Office will be implementing an Integrated Voice Response system that allows for call management and monitoring.

We will work with Callscan Australia Pty Ltd (QPC) to implement an IVR platform and this will entail having data stored and managed in the IVR platform, which is administered through a third-party cloud infrastructure, addressing the risks identified and discussed below.

The key risks centre on the security and storage of information on cloud servers overseas and accidental disclosure of personal information by the Office, QPC and third party suppliers, rather than external access. Recommendations to address risk are set out below, including communication and monitoring of QPC and third party supplier's compliance with the contract and APP 11 (security of information) and APP 8 (cross-border flow of information).

PIA methodology

Consultation:

- ICT and Security – Director and Assistant Director
- QPC – Account Manager, Project Manager and Technical Support Specialist
- Legal Team
- BIIP – Director
- Complaints – Director

Review:

- *Privacy Act 1988* (Cth)
- Australian Privacy Principles
- Office of the Commonwealth Ombudsman Privacy Policy
- Office of the Commonwealth Ombudsman Privacy Breach Policy
- Office of the Commonwealth Ombudsman Privacy Management Plan
- Office of the Commonwealth Ombudsman Data Breach Policy
- QPC ISMS User Access Management Standard (governs accessing their systems, which include the IVR platform.

Stakeholders:

- Members of the Public
- Office of the Commonwealth Ombudsman staff
- Office of the Commonwealth Ombudsman customers and clients
- Australian Government departments, agencies and authorities
- Digital Transformation Authority
- Callscan Australia Pty Ltd ('QPC')
- Public Health Insurance Operators
- Postal Operators
- Education Service Providers
- Police agencies
- Immigration authorities
- Third-party cloud provider
- The platform provider

Project Overview

This PIA relates to the project titled 'Integrated Voice Response (IVR) Implementation.'

The Office is currently using two systems for inbound and outbound telephony: Microsoft Teams and NEC TouchPoint (Desktop).

The Office requires an IVR scalable to future service requirements. In December 2022 the Office signed a contract with QPC, a company based in Victoria, Australia, which is a partner ('Authorised Organisation') of the company who administers the IVR platform

This procurement comprises the configuration and deployment by QPC of the IVR platform, which will be hosted on a third party platform.

QPC has deployed a project team to work with the Office's Project Director and Project Manager (and through them, the Project Sponsor and Key Project Stakeholder) to undertake analysis, design, provisioning, configuration, consultation and deployment of the agreed IVR platform.

The aim of the initial implementation is to retain current inbound/outbound call functionality and associated phone numbers/lines, and to:

- introduce inbound and outbound calling functionality for 'Agents' (i.e. staff licensed to the IVR platform) working from home or working in any of our Office locations
- introduce minor improvements to the content and sequence of IVR messages heard by those making inbound calls to the designated phone lines, call/call back queues and flows (see Table 1 below)
- introduce real-time and historical reporting on call activity at the queue, queue branch, agent and whole-of-operation levels
- enable workflow setup through IVR prompts to deliver callers to Agents or groups of Agents
- introduce real-time and historical reporting on call pathways for all call outcomes
- support the potential integration of call reporting data with Power BI

The responsible Project Director is Director, Business Intelligence, Improvement and Performance (BIIP), who reports to the Chief Operating Officer, Corporate Branch. The Project Director is supported by the Project Manager, Chief Information Officer and Director – Complaints.

A separate governance framework sets out the roles and responsibilities of the project's key internal stakeholders, including across the Office' executive, ICT and Legal teams, and operational stakeholders.

Personal Information Flows

The *Privacy Act 1988* (Cth) defines personal information as information or opinion about an ***identified individual***, or an ***individual who is reasonably identifiable,*** (whether the information or opinion is true or not, or whether the information or opinion is recorded in material form or not): s 6. It also includes information, that, if viewed in context and collated and taken together may make an individual identifiable. It is not information that does not identify an individual, for example, intellectual property, IT information, data that does not identify an individual, or corporate information about a company.

The key privacy elements of implementation relate to the real-time collection and storage of the information set out in the following Table 1. The personal information flows are also depicted in Table 1 and elaborated upon below. Material that is underlined would or could be considered personal information.

Call logs are retained until our Office no longer has an account with the IVR platform provider, that is, currently indefinitely. There are appropriate controls in place, reliant on anyone accessing the system to use Single Sign On. Information contained in Call Log is not sufficient to identify specific details with regard to an individual's interaction with the Office. Call Logs capture the following:

- Telephone Number
- Menu option selected
- Call duration

Call recordings, or an equivalent transcription, will be retained consistent with the Office's Records Authority. Recordings relating to out of jurisdiction and lower complexity work may be retained on the IVR platform. Recordings relating to higher category approaches will be transferred to our complaints and case management system and records system for retention. This complies with the *Archives Act 1983* (Cth) and the relevant Ombudsman's Records Authority. Call recordings can be both edited and deleted if required. Call recordings capture the following:

- Telephone Number
- Menu option selected
- Call duration
- Name
- Date of birth
- Address
- Email address
- Other personal details disclosed in lodging their complaint/raising their concerns, including but not limited to:
  - agency/organisation they engaged with
  - nature of their complaint, including decisions, documents, sensitive and private issues

- reference numbers, including a Reference Number given by the Office's Customer Relationship Management (CRM) system, client reference numbers used by other agencies to identify the client may include details like the above for family members or other members of the public discussed by the complainant.

Retention of chat records will be stored to an individual profile, and are retained until our Office no longer has an account with the IVR platform, that is, currently indefinitely. The contents of a Chat will be stored against the Profile of any User who is a participant in that Chat. The Chat data is not recorded against the call interaction it relates to. The chat data cannot be deleted from the system. Agents will be given written instructions and refresher training on the appropriate use of the Chat function. The Office will monitor compliance by random audits and feedback as required.

<table>
<tr><th colspan="2">Table 1: Real-time collection and storage of information: Key privacy elements</th></tr>
<tr><td colspan="2">Designated Office phone lines: Data to be collected in real time and stored for every phone call inbound to the designated phone lines</td></tr>
<tr><td>Commonwealth Ombudsman Main line: 1300 362 072

Commonwealth Ombudsman Main – Defence Abuse Liaison (Direct Line): 1300 395 776

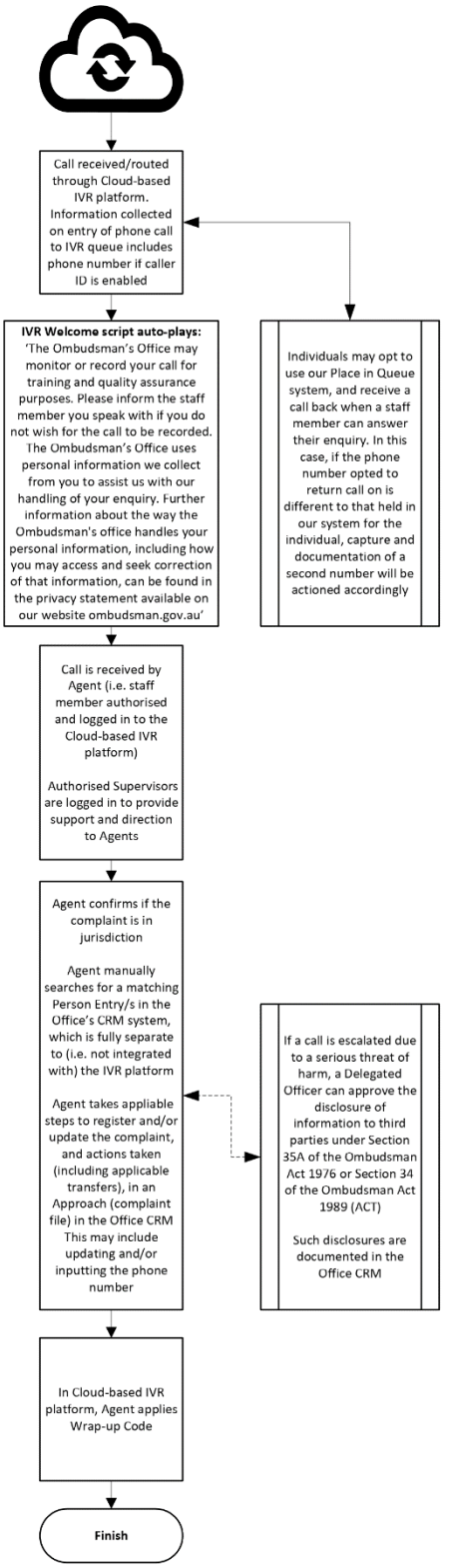
Indigenous (Direct Line) – 1800 060 789

ACT Ombudsman (Direct Line) – 02 5117 3650</td><td>IVR SYSTEM ONLY:
Telephone Number
Menu option selected
Call duration
May include the use of the Chat and Agent Assist functions (live chat in the IVR platform), which will include information relating to live calls, our processes and may reference some of the personal information detailed in the ‘CALL RECORDING’ section below; those recordings will be stored indefinitely on the IVR platform or its archives. The data collected would be stored in an encrypted manner. the IVR platform uses encryption keys that are unique for each organisation.
CALL RECORDING:
In addition to the above (‘IVR SYSTEM ONLY’), may include:
name
date of birth
address
email address
other personal details disclosed in lodging their complaint/raising their concerns, including but not limited to:
agency/organisation they engaged with
nature of their complaint, including decisions, documents, sensitive and private issues
reference numbers, including a Reference Number given by the Office’s CRM system, client reference numbers used by other agencies to identify the client
may include details like the above for family members or other members of the public discussed by the complainant.</td></tr>
<tr><td colspan="2">Outbound phone calls: Data to be collected in real time and stored for every outbound phone call made from the IVR platform
All information listed under ‘IVR SYSTEM ONLY’ and ‘CALL RECORDINGS’ in the immediately preceding cell applies, excepting ‘Menu Option Selected’ data, which is not collected when phone calls are made from the IVR platform.</td></tr>
</table>

Figure 2: Collection, storage and use of phone numbers

Figure 2 depicts information flows for the collection, use and storage of phone numbers in the Cloud-based IVR platform as configured for the Office of the Commonwealth Ombudsman.

Collection, storage and use of phone numbers
This Figure depicts information flows for the collection, use and storage of phone numbers in the Cloud-based IVR platform as configured for the Office of the Ombudsman



Information received and input into the Cloud-based IVR platform is stored in an encrypted manner, access to which is provided on the basis of business need. The Cloud-based IVR platform is protected against unauthorised access to the data through use of an encryption key unique to the Ombudsman's account.

Call recordings will be configured to be stored in a data centre located in Asia Pacific (Sydney). When call recording commences, phone numbers will also be available and expressly stated by the Agent, for both existing and new complaints

The Office is responsible for the security of user credentials used for accessing the IVR platform. Permission Levels will be assigned by virtue of group membership, managed by the Complaints area QPC will implement a single sign-on connector, which allows authorised Office users to log in to the IVR platform using their network credentials. The QPC User Access Management Standard – Information Security Management System documents how QPC will ensure the security of settings and credentials used in their capacity as an Authorised Organisation (partner) of the IVR platform.

Privacy Impact Analysis

The scope of this project requires the collection and storage of customer information as (outlined in Table 1 and Diagram 1 above) follows:

IVR system only

- Telephone Number
- Menu option selected – not personal information
- Call duration – not personal information
- May include the use of chat and agent assist functions (live chat in the IVR platform) which will include information relating to live calls, our processes and may reference some of the personal information also detailed in the call recording details below. The contents of a Chat will be stored against the Profile of any User who is a participant in that Chat. The Chat data is not recorded against the call interaction it relates to. The chat data cannot be deleted from the system and will auto delete when the Office no longer engages the services of the Platform provider. The data collected will be stored in an encrypted manner. The IVR platform uses encryption keys that are unique for each organisation.

Call recording

In addition to above, personal information may include:

- Name
- Date of birth
- Address
- Email address
- Other personal details disclosed in lodging their complaint/raising their concerns including but not limited to:
  - Agency they engaged with
  - Nature of their complaint, including decisions, documents, sensitive and private issues
  - Reference numbers, including OCO database reference number, client reference numbers used by other agencies to identify the client
  - May include details like the above for family members or other members of the public discussed by the complainant.

Compliance check

APP 1 — Open and transparent management of personal information

APP entities must have ongoing practices and policies in place to ensure that they manage personal information in an open and transparent way.

Have reasonable steps been taken to implement practices, procedures and systems that will ensure compliance with the APPs and any binding registered APP code for the purposes of the project?

See the OAIC's Privacy Management Framework for the steps the OAIC expects you to take to meet your obligations under APP 1.2. Agencies should also consider their obligations under the Privacy (Australian Government Agencies – Governance) APP Code 2017. Consider whether any adjustments or additions need to be made to your practices, procedures and systems for the purposes of this project.

The Office has policies for privacy that give effect to the APPs. For example, the Privacy Policy (9 September 2019) addresses the collection of personal information, the holding use and disclosure of such information in accordance with the APPs. The APPs relevantly govern the collection, use, storage, security and disclosure of personal information.

Privacy Breaches or breach of the APPs must be actioned in accordance with the Office's Privacy Breach Policy (January 2019), which makes provision for detecting, reporting and actioning privacy breaches, including notifying eligible data breaches to the Office of the Australian Information Commissioner (OAIC). Complaints and inquiries about the Office's compliance with privacy, including in relation to the IVR system, can be made in accordance with the Privacy Policy and Privacy Act.

The Office registers into the case management system contacts and complaints received by phone. IVR Implementation will not change this process.

The IVR platform is not integrated with Case Management Systems.

The Project Team and key internal stakeholders agree on the importance of the 'Four Steps' of the OIAC Privacy Management Framework: Embed, Establish, Evaluate, Enhance.

IVR Implementation will change the technology through which inbound calls are received and outbound calls made. IVR Implementation will also introduce the following new practices for some aspects of our business:

a) Automatically collecting the following data for every inbound and outbound phone call:

- Phone number a call was delivered from (inbound) or made to (outbound)
- Time a call was delivered (inbound) or made (outbound)
- Date a call was delivered (inbound) or made (outbound)
- Call duration
- IVR menu option/s selected (only inbound)
- Wrap-Up codes are manually recorded against each 'Interaction' by authorised Users.

b) Automatically storing the following data for every inbound and outbound call:

- Phone number a call was delivered from (inbound) or made to (outbound)
- Time a call was delivered (inbound) or made (outbound)
- Date a call was delivered (inbound) or made (outbound)

- Call duration
- IVR menu option/s selected. (only inbound)
- Wrap-up Codes manually recorded against each 'Interaction'

If call recording is introduced (a) and (b) will collect and store the following in addition to that set out above:

- Name
- Date of birth
- Address
- Email address
- Other personal details disclosed in lodging their complaint/raising their concerns including but not limited to:
  - Agency they engaged with
  - Nature of their complaint, including decisions, documents, sensitive and private issues
  - Reference numbers, including Office database reference numbers, client reference numbers used by other agencies to identify the client
  - May include details like the above for family members or other members of the public discussed by the complainant.

c) Collecting and regularly renewing, via approved synchronisation through Microsoft Azure Active Directory, the following data:

- For Authorised Users (Agents, Supervisors and Administrators): first name, last name, email address and Office contact phone number (Microsoft Teams direct lines)
- For other Office staff accessible through Microsoft Azure Active Directory: first name, last name, email address and Office contact phone number (Microsoft Teams direct lines)

d) Manually collecting, updating and storing until deleted:

- first name, last name and phone number of individuals external to the Office
- organisation name and phone number of organisations external to the Office

Our case management system is the central repository in which phone numbers identified or identifiable to individuals or organisations are collected, stored and updated, as part of the registration of complaints/contacts and ongoing complaints case management. This meets the requirements for security as required under the *Archives Act 1983* (Cth) in relation to the secure storage of records.

Within the IVR platform, phone numbers are collected immediately as a call is delivered or made. This numeric data is not matched to individuals or organisations (unless manually collected – see (d) above. However, it is possible that authorised Users may use phone numbers collected and stored in the IVR platform to cross-search for Person Entries or Approaches within the Office's CRM system.

If an Agent needs to write to authorised User/s in the IVR platform (e.g. a Supervisor, or another Agent) for help or advice, they may do so using the Chat function. The contents of a Chat will be stored against the Profile of any User who is a participant in that Chat. The Chat data is not recorded against the call interaction it relates to. Agents will be given written instructions on the appropriate use of the Chat function.

Do you have an APP privacy policy which:

- **is clearly expressed, understandable and up-to-date**
- **covers the matters listed in APP 1.4**
- **is freely available at no cost (for example, on your website).**

Identify the document(s) and provide a link where available or include as an attachment to this PIA. See the OAIC's *Guide to developing an APP privacy policy* for more information.

The Office of the Commonwealth Ombudsman Privacy Policy is accessible to members of the public at no cost from Privacy Policy | Commonwealth Ombudsman.

In addition, the Office has the following Privacy Policies, which are regularly reviewed and updated:

- Privacy Policy
- Privacy Breaches Policy
- Privacy Impact Assessment Template
- Privacy Impact Assessment Guidelines
- Privacy Management Plan
- Data Breach Response Plan

Will the APP privacy policy need to be updated to reflect a new collection, use or disclosure of personal information for the purposes of this project?

Your analysis under APP 3 and APP 6 should inform whether updates to your entity's APP privacy policy are required (see below).

Our Privacy Policy covers how we collect and disclose information and considers how data will be used. The IVR platform does not alter how we collect, use of disclose information.

The Office's Privacy Policy reflects and complies with its obligations under the Privacy Act and APPs. The policies will be reviewed to align with the requirement of this project, noting that coverage of third party obligations of privacy are limited, and supplemented by the legislation, APPs, and the contractual obligations of QPC with regard to privacy and storage and security of personal information.

Are there procedures and systems in place for handling privacy inquiries and complaints?

Identify the process (internal and external) for making a privacy inquiry or complaint, including who is responsible for complaint handling. Is it visible, comprehensive and effective?

External – As per Office of the Ombudsman website Privacy Policy | Commonwealth Ombudsman

How do I complain about the handling of my personal information

We are committed to protecting your personal information. If you are concerned about the Office's handling of your information, you may submit your complaint in writing using our online complaint form. You can also call **1300 362 072** and ask to speak with a Privacy Officer.

Internal – As per Office of the Ombudsman intranet

Suspected privacy breaches

If you become aware, in the course of your work, that there may have been a breach of privacy (whether deliberate or inadvertent) by the Office, then you should report this immediately to your supervisor, who will refer it for investigation and/or advice from the Legal Team. Legal Team members are designated 'Privacy Contact Officers' and can provide you with advice and assistance in relation to any questions you may have about the Office's obligations under the Privacy Act.

If you receive a complaint about a breach of privacy by the Office then this should also be referred to the Legal Team - see APP 1 above.

The main documents dealing with systems for handling privacy inquiries and complaints are the Office's:

- Privacy Policy
- Privacy Breaches Policy

APP 2 — Anonymity and pseudonymity

Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter, unless an exception applies.

Will individuals have the option of not identifying themselves or of using a pseudonym? If not, explain why it is impracticable for you to deal with individuals who have not identified themselves or who have used a pseudonym.

Describe how individuals will be provided with the option of not identifying themselves or of using a pseudonym. Alternatively, explain why it is impracticable for you to deal with individuals who have not identified themselves (for example, if you need to deliver purchased goods to an individual, you may need to know their name if the individual needs to sign for delivery). See Chapter 2 of the APP Guidelines for more information about when it may be impracticable to deal with an individual who is not identified.

Our Privacy Policy on the Office's website (Privacy Policy - Commonwealth Ombudsman) states:

"You may complain to us anonymously or by adopting a pseudonym. However, if you do so it may be difficult or impossible for us to investigate your complaint."

In relation to the collection of information on the IVR systems, users and callers will have the option to identify themselves anonymously and using a pseudonym, subject to the requirements of the Privacy Act and relevant legislation, regulations and laws where a person is required to identify themselves, for example, to request access to personal information."

It is noted that callers will not have the option to de-identify the phone number they are calling from under the IVR. If they are not calling from a private or restricted number, the incoming phone number will be captured, stored and recorded.

Are you required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves?

Identify the law that requires or authorises you to deal with identified individuals.

Yes, occasionally the Office is required to establish the identity of persons or proof of identity in order to deal with them under the provisions of the Office's governing legislation, the *Ombudsman Act 1976* (Cth). Section 35 of the Ombudsman Act prohibits the disclosure of information about complainants by officers of the Office. Such information could only be disclosed in the course of investigations to identified individuals under the relevant exceptions to disclosure in the Ombudsman Act. The Office also, for example, requires persons to establish their identity in order to make a request for access under the *Freedom of Information Act 1982* (Cth) and/or *Privacy Act 1988* (Cth).

Are there categories of individuals affected by the project who are likely to seek to interact with your entity anonymously or using a pseudonym?

For example, an individual may prefer to deal anonymously or pseudonymously with you for various reasons including to access services (such as counselling or health services) without this becoming known to others, or to keep their whereabouts secret from a former partner or family member.

For an initial contact, where the individual is not seeking to lodge a complaint, engaging us on a matter that is out of our jurisdiction or not expecting an outcome, we do not need to obtain personal details in some instances and therefore the individual need not identify themselves, for example when an individual contacts us about a matter that is quickly identified on the phone that it not in the jurisdiction of the Office. General advice and information can also be provided to members of the public who contact the Office.

Outside of this circumstance, an individual will need to identify themselves. A small number of clients choose to remain anonymous and internal processes allow for this. Personal information will not be disclosed to other persons other than in accordance with law.

To comply with confidentiality obligations under the *Ombudsman Act 1976* (Cth), an individual caller will usually need to identify themselves and provide sufficient Proof of Record Ownership when discussing personal details and complaint specifics.

APP 3 — Collection of solicited personal information

Any personal information collected (other than sensitive information) must be reasonably necessary for (or if your entity is an agency, reasonably necessary for, or directly related to) one or more of the entity's functions or activities.

An APP entity must not collect sensitive information about an individual unless one of the exceptions listed in APP 3.3 or APP 3.4 applies.

Personal information can only be collected by lawful and fair means.

Personal information about an individual must only be collected from the individual unless one of the exceptions in APP 3.6 applies.

If you are an agency, is the information being collected necessary for, or directly related to, one or more of your functions or activities?

If you are an organisation, is the information being collected necessary for one or more of your functions or activities?
List each item of personal information that will be collected (eg. name, date of birth, address) and explain why each item is necessary for one or more of your functions or activities. This should be a very granular assessment. You should clearly and specifically describe the relevant function or activity and why each item of personal information is reasonably necessary for (or, for agencies, directly related to) that specific function or activity. You should only collect the minimum amount of personal information that is necessary for the relevant function or activity ('data minimisation').

Data minimisation is an important concept that can help reduce the privacy impacts for individuals that may be associated with your project. Minimising the amount of data that you collect can also help to mitigate security risks. For example, collecting more personal information than is necessary may increase the risk of harm to an individual in the event of a data breach, which could also trigger your notification obligations under the Notifiable Data Breach scheme. Holding large amounts of personal information may also increase the risk of unauthorised access by internal or external sources. Security issues are considered further below under APP 11.

Also consider whether your APP privacy policy will need to be updated if the project will involve a new collection of personal information and record this under APP 1 above.

Privacy risk: If some personal information is not reasonably necessary for the project, there may be a risk of over collection. For example, it may be not be necessary to collect all personal information on an individual's driver licence when the purpose of collection is to verify the individual's age.

The personal information collected as identified above in this report includes:

IVR system only

- Telephone Number
- Menu option selected – not personal information
- Call duration – not personal information
- May include the use of chat and agent assist functions (live chat in the IVR platform) which will include information relating to live calls, our processes and may reference some of the personal information also detailed in the call recording details below. These recordings will be stored indefinitely on in the the IVR platform or it's archives. The data collected will be stored in an encrypted manner. The IVR platform uses encryption keys that are unique for each organisation.

Call recording

In addition to above, personal information may include:

- Name
- Date of birth
- Address
- Email address
- Other personal details disclosed in lodging their complaint/raising their concerns including but not limited to:
  - Agency they engaged with
  - Nature of their complaint, including decisions, documents, sensitive and private issues
  - Reference numbers, including OCO database reference number, client reference numbers used by other agencies to identify the client
  - May include details like the above for family members or other members of the public discussed by the complainant.

The collection of this information is necessary for the Office to discharge its functions under the *Ombudsman Act 1976* (Cth), including to investigate complaints regarding a matter of administration in relation to the actions of government and other agencies and to conduct own motion investigations where appropriate. Individuals can lodge a complaint with the Office, and the Ombudsman must investigate such complaints.

For the collection of sensitive information, can you rely on any of the exceptions in APP 3.3 or APP 3.4?

Explain which exception you are relying on for the collection of any sensitive information. For example, has the individual consented or is the collection required or authorised by or under an Australian law or a court/tribunal order?

Yes, the collection of sensitive information from our users, clients and complainants is necessary for the agency to discharge its functions under the *Ombudsman Act 1976* (Cth), including s 5 and s 8 relating to the investigation of complaints and it is reasonably necessary for the Office's functions. Sensitive information includes information or an opinion about an individual's:

- racial or ethnic origin
- political opinions or associations
- religious or philosophical beliefs
- trade union membership or associations
- sexual orientation or practices
- criminal record
- health or genetic information

Parts A and B of the Privacy-Policy-September-2019.pdf (ombudsman.gov.au) confirms the legal basis upon which the collection of information, including sensitive information, is necessary for/directly related to the Ombudsman's functions.

Will the information be collected by lawful and fair means?

Describe the means by which personal information will be collected.

⚠ **Privacy risk**: Your method of collection may be 'unfair' if it involves intimidation, deception or is unreasonably intrusive. For example, it would usually be unfair to collect personal information covertly without the knowledge of the individual (however, this will depend on the circumstances).

The means of the collection of information by the Office, through QPC as contractor, will be lawful and fair. It will be collected in accordance with our Privacy-Policy-September-2019.pdf (ombudsman.gov.au) which specifies the manner in which the Ombudsman collects information.

Specifically, we will collect personal information from the person it relates to or their authorised representative from a telephony interaction.

As allowed by the *Ombudsman Act 1976* (Cth) and law, we will collect information from a third party or authority to allow us to resolve customer's complaint.

We notify the customer of collecting of information in our welcome messaging, which states your call may be monitored for quality or training purposes. When call recording is activated, this message will be retained and the calls will not be utilised in any other manner, apart from where provided for by relevant legislation.

Will the personal information be collected from the individual concerned? If not, do any of the exceptions in APP 3.6 apply?

Describe how, and from which other sources, the personal information will be collected. Also, explain which exception you are relying on to collect personal information about the individual from another source.

⚠ **Privacy risk**: There may be a risk of the information being inaccurate, out-of-date or incomplete if collected from another source.

The data will be collected from individuals, their authorised representatives (termed 'On Behalf Of') and a range of other agencies and organisations whose numbers are inbound or outbound to or from the IVR platform and whose information is recorded.

The individuals have either expressly or impliedly consented to the collection of information under APP 3.6 by the Office, and its contractors, when they provide consent to use and record their information at the beginning of a call.

We notify our customers at the commencement of their call currently that their call may be recorded or monitored:

> "The Ombudsman's Office may monitor or record your call for training and quality assurance purposes. Please inform the staff member you speak with if you do not wish for the call to be recorded. The Ombudsman's Office uses personal information we collect from you to assist us with our handling of your enquiry. Further information about the way the Ombudsman's office handles your personal information, including how you may access and seek correction of that information, can be found in the privacy statement available on our website **www.ombusman.gov.au**"

If the collection of personal information will be outsourced, will measures be in place to ensure compliance with APP 3and prevent over collection of information?

Describe how you will ensure that any third party that collects personal information on your behalf complies with APP 3 (for example, by entering an enforceable contractual arrangement).

The Office collects only what is necessary to discharge its functions under the *Ombudsman Act 1976* (Cth). Over collection will be prevented at first instance by only collecting information relevant to a complaint in accordance with the complaints officer's statutory obligations and Complaints Handling Procedure and Manuals. Secondly, it will involve storing that information security on case and records management systems and proper training of staff.

The design, configuration, implementation and ongoing maintenance of the IVR platform is delivered to the Office (under an enforceable Contract) by QPC, which is an Authorised Organisation (partner) of the platform provider. In turn, the platform provider uses third-party cloud infrastructure for encrypted relay and storage of data collected as a result of the Office's use of the platform. It is only a product used to collect information and not the content or substantive information as such.

It is important to state in this Privacy Impact Assessment that the underlying product development by the platform provider is intensive and continual. Nevertheless, the Office is the buying client in this arrangement, and must agree and remain informed of the type/s of personal information collected and stored within the platform.

APP 4 — Dealing with unsolicited personal information

Where an APP entity receives unsolicited personal information, it must determine whether it would have been permitted to collect the information under APP 3. If so, APPs 5 to 13 will apply to that information. If the information could not have been collected under APP 3, and the information is not contained in a Commonwealth record, the APP entity must destroy or de-identify that information as soon as practicable, but only if it is lawful and reasonable to do so.

Are there practices, procedures and systems in place for dealing with the receipt of unsolicited personal information that will ensure compliance with APP 4?

As per Privacy-Policy-September-2019.pdf (available at www.ombudsman.gov.au) - In some circumstances, such as in the course of an investigation, we are given personal information about a person (which may be about someone other than the person who made the complaint), and we have not asked for this information. This is called 'unsolicited personal information' and can be provided by the complainant, an agency or another person. In these circumstances we will assess whether we would be permitted under the APPs to collect this sort of information from the person whose personal information it is. If we could have collected it from that person because of our functions and activities, then we will retain it, otherwise we will destroy it. We will not use or disclose unsolicited personal information unless this is permitted by the APPs. We will endeavour to tell you if we collect solicited or unsolicited personal information about you from someone else, however in some circumstances this will be not be reasonable for us to do. Due to the confidential nature of Ombudsman investigations we cannot disclose that a person has made a complaint to the Ombudsman.

APP 5 — Notification of the collection of personal information

An APP entity that collects personal information about an individual must take reasonable steps to notify the individual, or otherwise ensure the individual is aware, of the matters listed in APP 5.2.

An APP entity must provide notification before, or at the time it collects personal information. If this is not practicable, notification should be provided as soon as practicable after collection.

Consider each of the matters listed in APP 5.2. Will steps be taken to notify the individual of each matter? If steps are not being taken in relation to a matter, is it reasonable not to notify the individual?

Describe the steps taken to notify the individual OR explain why steps are not being taken. Include a link or attach collection notices where appropriate.

We notify our customers at the commencement of their call currently that their call may be recorded or monitored:

> "The Ombudsman's Office may monitor or record your call for training and quality assurance purposes. Please inform the staff member you speak with if you do not wish for the call to be recorded. The Ombudsman's Office uses personal information we collect from you to assist us with our handling of your enquiry. Further information about the way the Ombudsman's office handles your personal information, including how you may access and seek correction of that information, can be found in the privacy statement available on our website www.ombusman.gov.au>"

In addition to the above, the Office will take steps to notify an individual (under APP5.2):

- of its identity and contact details, where information collected is not directly from the individual
- if collection is require or authorised by law or court or tribunal order
- of the purpose for which it collects information
- of the consequences for the individual if information is not collected
- to of applicable APP privacy policies binding on it; and
- whether information is likely to be disclosed to overseas recipients and the countries where located, where it is reasonable in the circumstances.

If personal information is collected from another source, will the individual be notified? What steps will be taken to notify of each of the APP 5.2 matters?

Describe the steps taken to notify the individual OR explain why steps are not being taken. Include a link or attach collection notices where appropriate.

Privacy risk: If you are collecting personal information from another source, there may be a risk that an individual is not aware that you have collected their personal information. Ensure that any third-party notifies, or makes an individual aware, of the relevant APP 5 matters on your behalf (such as through an enforceable contractual arrangement).

By definition, many of complaints we receive require us to engage directly with the Agency or prescribed organisation being complained about. The Ombudsman collects personal information from complainants and other third parties in the course of performing its functions under the ***Ombudsman Act 1976*** (Cth). Where this is collected from another source other than call recordings the party would be notified if use was being made of that information, either throughout the complaint process or during the call.

APP 6 — Use or disclosure of personal information

An APP entity can only use or disclose personal information for the particular purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies, such as where the individual has consented to the use or disclosure of the information.

Note that APP 6 does not apply to organisations using or disclosing personal information for the purpose of direct marketing (refer to APP 7), or government related identifiers (refer to APP 9).

Does the project use or disclose personal information (including sensitive information) for a secondary or additional purpose?

Describe the secondary purpose and explain how it is authorised, by either asking the individual to consent, or by applying one of the exceptions to the requirement for consent in APP 6.2. Also consider whether your APP privacy policy will need to be updated if the project will involve a new use or disclosure of personal information and record this above under APP 1.

The IVR project intends to use personal information in the ways and methods described above at Table 1. The primary purpose will be for the use of Ombudsman to fulfil and discharge its statutory functions under the *Ombudsman Act 1976* (Cth), including to investigate complaints relating to administrative action. This is the primary purpose of making, receiving and recording calls. A secondary purpose may be permitted for lawful purposes, such as to comply with legislative obligations or court or tribunal orders. For example, compliance with court summonses. It is noted the Ombudsman is non-compellable and immune from suit. Some limited sensitive information may be collected, for example, relating to a caller or complainant's health circumstances. The Office's current Privacy Policy and Privacy Breaches Policy adequately protects such information.

If you are an agency, is it possible that personal information may be used or disclosed because it is reasonably necessary for an enforcement related activity? If so, are procedures in place to ensure a written note of the use or disclosure is made in compliance with APP 6.5?

Section 35A of the *Ombudsman Act 1976* (s 34 of the ACT Act) allows the Office to disclose personal information in response to a serious threat of harm where it is in the public interest.

This is a broad discretion. It is most commonly used within the Office:

- to disclose information to the state police or mental health services where a threat of self-harm or threat of harm to others is received, or
- to disclose that information to the relevant agency or a person within that agency where a threat of harm to another agency is received.

These are examples only and do not limit the exercise of the discretion by the delegate. It is not a list of circumstances to guide escalation of issues. Delegates exercise judgement on a case-by-case basis to determine whether disclosure is warranted, with consideration to the circumstances and nature of the threat, and the person's particular circumstances.

Will the individual be notified of any additional use(s) or disclosure of their personal information?

Explain how the individual will be given notice of the secondary use(s) or disclosure of their information, or why notice is not required (eg. additional notice may not be required if the proposed use or disclosure is consistent with the notice originally provided at the point of collection).

⚠ **Privacy risk**: If relying on APP 6.2(a) to use or disclose personal information for a secondary purpose, but your project involves a new way of handling personal information, there may be a risk that individuals would not reasonably expect their personal information to be used for the new purpose. Carefully consider whether additional notification is required.

Yes individuals will be notified if there is a breach of the Privacy Policy, a breach of the Privacy Act, a breach of the APPs, a serious infringement of privacy or an eligible data breach that is notifiable to the Office of the Australian Information Commissioner under the *Privacy Act 1988* (Cth). QPC also has contractual obligations to notify the Office in the event of the unauthorised disclosure of an individual's personal information.

If you're disclosing personal information to another entity (eg. if you are outsourcing some of your functions, or as part of an ongoing data sharing arrangement), will measures be put in place to protect the information and will compliance with APP 6 be monitored?

Describe the measures (such as an enforceable contractual arrangement or other information sharing agreement) that will be put in place to ensure compliance with APP 6 and protect the personal information that is being disclosed/shared. If no measures will be put in place, explain why (for example, the disclosure is a once-off and permitted by one of the exceptions under APP 6).

As noted above in the Overview, and Privacy Impact Analysis, the Office has a Privacy Policy and Privacy Breaches Policy in place. The outsourcing functions are governed by the Office's Short Form contract with QPC and the Head Agreement with the Digital Transformation Authority. These relevantly include provisions for the confidentiality, storage, privacy breach, privacy action, claims, insurance, subjugation and other provisions to ensure protection of privacy. QPC was required to take data protection measures, hold relevant insurances, and ensure safe and secure storage of information. QPC must report privacy breaches or unauthorised use under its contractual obligations specified in the contract.

APP 8 — Cross-border disclosure of personal information

Before an APP entity discloses personal information to an overseas recipient, the entity must take reasonable steps to ensure that the overseas recipient does not breach the APPs (other than APP 1) in relation to the information, unless an exception applies, such as the individual has given informed consent.

An APP entity that discloses personal information to an overseas recipient is accountable for any acts or practices of the overseas recipient in relation to the information that would breach the APPs (see s 16C of the Privacy Act).

Will any personal information be disclosed to an overseas recipient?

Describe what information will be transferred, to whom the information will be transferred, in which jurisdiction the information will be stored, and how the information will be transferred.

- Yes, as outlined above in the Project Overview, Privacy Impact Analysis, personal information will be disclosed by the Office to QPC, and by QPC to its third party suppliers who provide the call recording platform and various cloud an IT storage systems.
- It has been agreed in the contract with QPC that data may be accessed by the IVR platform administrator's personnel from around the world for support, maintenance, and troubleshooting purposes to provide 24x7x365 coverage and maintain the functionality of its telecommunications systems.
- It is also noted in the contract with QPC that all domestic network traffic is routed exclusively through Australia. Email interactions in the Asia Pacific, Australia, and Japan regions are routed through the USA region. This is a transit activity only, with all email data stored in the Australian region.
- The Office has taken reasonable steps with the supplier to ensure that the overseas recipient does not breach the APPs in relation to the collection, use storage and disclosure of personal information in conformance with s 95B of the Privacy Act. QPC is a contracted service provider. The contract ensures compliance with privacy obligations, taking steps to mitigate risk and consequences for privacy breaches including a right to take action for breach against the supplier and to recover costs.

Will reasonable steps be taken under APP 8.1 to ensure the overseas recipient does not breach the APPs (other than APP 1) in relation to the information?

Explain the arrangements in place with overseas recipients to ensure that personal information is handled in accordance with the APPs. For example, provide details of any enforceable contractual arrangement.

As per the Telecommunications Marketplace Short Form Contract in place between the Office and Callscan Australia Pty Ltd, consistent with Commonwealth Government practice relevantly provides for the protection of the Office's material, including not to sell, transmit, store or communicate it outside Australia unless required for the contract. In the event information was stored overseas or transmitted through overseas servers, QPC and the IVR Platform provider will be required under the contract to encrypt data sent outside of Australia with Office approved cryptography and methods. The key required to decrypt the material would be stored in Australia.

Alternatively, does an exception under APP 8.2 apply?

Explain how one of the exceptions in APP 8.2 apply to the transfer. For example, is the disclosure required or authorised by or under an Australian law or a court/tribunal order?

Not applicable

APP 10 — Quality of personal information

An APP entity must take reasonable steps to ensure that the personal information it collects is accurate, up-to-date and complete.

An APP entity must take reasonable steps to ensure that the personal information it uses and discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

What steps will you take to ensure the personal information collected is accurate, up to date and complete? Will guidance or processes be in place to ensure these steps are followed?

Guidance is provided, as per the Office's Privacy Policy Privacy Policy | Commonwealth Ombudsman

> **'How can I access or correct my personal information held by the Ombudsman**
>
> If you wish to access personal information we hold about you, or to correct that personal information, you can
>
> - ask your current contact in the Office (eg your complaints officer) to update information such as your address or contact details
> - email your request to information.access@ombudsman.gov.au
> - mail your request to the 'Privacy Officer' GPO Box 442, Canberra ACT 2601
> - call 1300 362 072 and ask to speak with a Privacy Officer.'

Ensuring the appropriate use of Proof of Record Ownerships and updating details as per information provided by the owner of the information or identified through duration of call and permission gained by owner of the information to have their personal information updated.

Callers and complainants are able to correct their records and personal information under the *Freedom of Information Act 1982* (Cth) and *Privacy Act 1988* (Cth). They can correct or amend inaccurate records or recordings. The Office will take steps to ensure it contacts QPC or the IVR Platform provider to ensure correction of material.

What steps will be taken to ensure that any personal information being used or disclosed is accurate, current, complete and relevant, having regard to the purpose of the use or disclosure? Will guidance or processes be in place to ensure these steps are followed?

⚠ **Privacy risk**: Carefully consider the consequences for individuals if the personal information is not accurate or up-to-date, including the kinds of decisions made using the information and the risks of using or disclosing inaccurate information.

As above

APP 11 — Security of personal information

An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

Where an APP entity no longer needs personal information for any purpose for which the information may be used or disclosed under the APPs, the entity must take reasonable steps to destroy the information or ensure that the information is de-identified, unless an exception applies.

The OAIC's *Guide to Securing Personal Information* sets out the reasonable steps the OAIC expects entities to take to protect personal information.

Are there technical security measures in place to protect the personal information that will be collected, used and/or disclosed as part of this project?

Describe the technical controls (such as software security, encryption, whitelisting and blacklisting, backing up, email security etc) that have been, or will be, implemented for the project, including any relevant policies and procedures. Include links or attachments where appropriate.

Privacy risk: If there are inadequate technical security measures in place, consider whether there is a risk that the information will not be properly protected, leading to misuse, interference, loss, unauthorised access, modification or disclosure. Consider the nature of the personal information collected and how valuable it would be to unauthorised users?

The contract with QPC requires the data to be encrypted to the Office's satisfaction and relevantly stored in Australia where required. The Office only would have the ability to unencrypt the data. The data would be stored in an encrypted manner, which would require permissions to be provided to access the information. This would be on a business needs basis. IVR Platform Cloud uses encryption keys that are unique for each organisation. These encryption keys protect recordings from authorised access to the following information. Call recording are configured to be stored in a data centre located in Asia Pacific (Sydney). Call recordings are encrypted at rest.

The security of personal information presents the largest risk to privacy. APP 11 is therefore of critical importance. The Office must take steps to ensure its contracted supplier complies with its obligations to store personal information securely, in a way that prevents its unauthorised access from hackers. The greatest risk is that information could be misused and perhaps threats made to the Australian government and its agencies following the unauthorised use of such information.

Are there physical security measures in place to protect the personal information that will collected, used and/or disclosed as part of this project?

Describe the physical security measures that have been, or will be implemented, for the project, including any relevant policies and procedures. Include links or attachments where appropriate.

The data will be stored in an encrypted manner, which will require permissions to be provided to access the information. This would be on a business needs basis. the administrator of the IVR platform uses encryption keys that are unique for each organisation. These encryption keys protect recordings from authorised access to the following information. Call recording are configured to be stored in a data centre located in Asia Pacific (Sydney). Call recordings are encrypted at rest.

Are there access security and monitoring controls in place to protect against internal and external risks and ensure that personal information is only accessed by authorised persons?

Describe the access security controls (such as identity management and authentication, password practices, audit logs/trails and access monitoring) that have been, or will be, implemented for the project, including any policies and procedures. Consider who will have access to the data and ensure access is limited to those staff (or other third parties) necessary to enable your entity to carry out its functions and activities (ie. access should be strictly on a 'need-to-know' basis). Include links or attachments where appropriate.

Privacy risk: Inadequate access security and monitoring controls may lead to the 'trusted insider risk', which can occur when staff mishandle personal information while carrying out their normal duties.

The data would be stored in an encrypted manner, which would require permissions to be provided to access the information. This would be on a business needs basis. the administrator of the IVR platform uses encryption keys that are unique for each organisation . These encryption keys protect recordings from authorised access to the following information. Call recording are configured to be stored in a data centre located in Asia Pacific (Sydney). Call recordings are encrypted at rest.

QPC login to their own account using SSO and MFA then access our IVR platform via the Authorized Organizations link. QPC also maintain a direct login account on our Organisation but this will remain logged off, and turn on when QPC flag that they need it to provide support. This will remove any unnecessary security risk.

Documents and Processes governing Access Control:

- Information and Communications Technology Information Security Policy

QPC User Access Management Standard governs accessing our systems including our IVR platform organisation and account.

Have you completed a separate security risk assessment?

If so, please refer to or attach a copy of the assessment to this PIA.

The Chief Information Officer and IT Security Adviser have assessed that the solution implements suitable security controls to meet our privacy obligations. Notable controls are:

1. Australia-based hosting on an IRAP-certified cloud platform.
2. Ombudsman access is restricted to active staff using single sign on (SSO) on Office managed devices within Australia.
3. QPC and IVR Platform administrator access requires multi-factor authentication.
4. All administration user activities are logged and monitored.
5. Data encrypted in transit and at rest.

Have you considered standards that may apply to your industry or sector? If you have decided not to adopt a widely used standard, document your reasons below.

You should consider using relevant international and Australian standards, policies, frameworks and guidance on information security. This includes any which are particular to your sector or industry. Australian Government agencies must apply the Attorney-General's Department's Protective Security Policy Framework and the Australian Signals Directorate's Australian Government Information Security Manual.

You may also want to consult the ISO/IEC 27000 series of information security management standards and the ISO/IEC 31000 series of risk management standards published by both the International Organization for Standardization and the International Electrotechnical Commission, parts of which have been adopted by Standards Australia.

Initially, prior to introduction of call recording, we are compliant and aligned to Industry Standards. We notify our customers at the commencement of their call currently that their call may be recorded or monitored:

> "The Ombudsman's Office may monitor or record your call for training and quality assurance purposes. Please inform the staff member you speak with if you do not wish for the call to be recorded. The Ombudsman's Office uses personal information we collect from you to assist us with our handling of your enquiry. Further information about the way the Ombudsman's office handles your personal information, including how you may access and seek correction of that information, can be found in the privacy statement available on our website www.ombusman.gov.au."

With the introduction of call recording, we will consider, align and comply with Australian standards and legal obligations such as those listed in the *Privacy Act 1988* (Cth) and *Telecommunications (Interception and Access) Act 1979* (Cth).

If you have outsourced personal information handling as part of this project, what steps will be taken to ensure personal information is protected by third party providers?

Describe the measures (such as conducting due diligence on the services to be provided and contractual provisions relating to security requirements) that will be taken to ensure third party providers protect any personal information handled on your behalf.

⚠ **Privacy risk**: Failing to conduct appropriate due diligence on the services to be provided is inconsistent with your obligations under APP 11 and can lead to an increased risk of a data breach if the third-party provider does not have adequate security measures in place.

The two third-party providers are QPC and IVR Platform provider. The Office contract with QPC specifies provisions relating to security requirements, which QPC makes in its capacity as an Authorised Organisation of the IVR platform provider. The contract imposes storage and encryption obligations on the outsourced third party providers, including in relation to information stored on the cloud.

Do you have a data breach response plan in place? If so, describe at a high level the steps that you will take in the event of a data breach or attach your response plan.

See the OAIC's Notifiable data breaches page which sets out information to help APP entities prepare for and respond to data breaches. You should consider whether changes to your existing data breach response plan need to be made as a result of this project.

The Office has a Data Breach Response Policy.

In the event of a Data Breach we would follow the Key Step Plan listed within:

- Action – immediately notify the Privacy Officer – Legal Team
- Assess – Office Legal Team is responsible for conducting an assessment of the data breach. The assessment should be completed within 30 calendar days (s 26WH(2) Privacy Act) after OCO became aware there may be an eligible data breach.
- Notify – The NDBS requires the Office to notify individuals and the OAIC of 'eligible data breaches'. A data breach is eligible if it is likely to result in serious harm to any of the individuals to whom the information relates and where the Office has been unable to prevent the likely risk of serious harm with remedial action. There are three options for notifying individuals at risk of serious harm, depending on what is 'practicable' for Office. (s 26WL(2) Privacy Act).

Completion of the relevant Data Breach – Report would also be conducted.

QPC is also required under the contract to comply with obligations to report notifiable data breaches to the OAIC under the Privacy Act. They must notify the Office of any eligible data breaches within 48 hours of the breach occurring and, impliedly, provide assistance with providing any information necessary to notify an eligible data breach.

If you have outsourced personal information handling as part of this project, have you considered your obligations under the Notifiable Data Breaches (NDB) scheme and how you will manage your relationship with the third party?

Describe how you will ensure you comply with the NDB scheme in the event a third-party provider experiences a data breach (such as including contractual terms to allocate responsibility for identifying, assessing and notifying as required).

If a Data Breach was to occur by QPC or IVR Platform provider, they have established processes to notify of Data Breaches internally and to their clients. IVR Platform Provider Security and Compliance policies are published on their website.,

As noted, the Office has the following privacy policies to comply with the NDB Scheme:

- Privacy Policy
- Privacy Breaches Policy
- Privacy Impact Assessment Template
- Privacy Impact Assessment Guidelines
- Privacy Management Plan
- Data Breach Response Plan

Under the Privacy Breaches Policy, the Legal Team would report eligible data breaches that may occur in future under the IVR system to the OAIC in accordance with the Privacy Act.

In the event of a Data Breach the Office would follow the Key Step Plan listed within the Data Breach Plan:

- Action – immediately notify the Privacy Officer, Legal team.
- Assess – the Office Legal Team is responsible for conducting an assessment of the data breach. The assessment should be completed within 30 calendar days (s 26WH(2) Privacy Act) after the Office became aware there may be an eligible data breach.
- Notify – The NDBS requires the Office to notify individuals and the OAIC of 'eligible data breaches'. A data breach is eligible if it is likely to result in serious harm to any of the individuals to whom the information relates and where the Office has been unable to prevent the likely risk of serious harm with remedial action. There are three options for notifying individuals at risk of serious harm, depending on what is 'practicable' for the Office. (s26WL(2) Privacy Act).

Completion of the relevant Data Breach – Report would also be conducted.

How long will you retain the personal information collected, used and/or disclosed as part of this project?

Describe any relevant retention and disposal schedules or policies.

Call logs are retained until our Organisation no longer has an account with the IVR platform, that is, currently indefinitely. There are appropriate controls in place, reliant on anyone accessing the system to use Single Sign On. Information contained in Call Log is not sufficient to identify specific details with regard to an individual's interaction with the Office. Call Logs capture the following:

- Telephone Number
- Menu option selected
- Call duration

Call recordings, or an equivalent transcription, will be retained consistent with the Office's Records Authority which can be found here: Office of the Commonwealth Ombudsman RA (naa.gov.au). Recordings relating to out of jurisdiction and lower complexity work may be retained on the The IVR platform. Recordings relating to higher category approaches will be transferred to our complaints management system for retention. This complies with the *Archives Act 1983* (Cth) and the relevant Records Authority of the Office of the Commonwealth Ombudsman 2008/00422945 – 30 September 2008.

Call recordings capture the following:

- Telephone Number
- Menu option selected
- Call duration
- name
- date of birth
- address
- email address
- other personal details disclosed in lodging their complaint/raising their concerns, including but not limited to:
    - agency/organisation they engaged with
    - nature of their complaint, including decisions, documents, sensitive and private issues
    - reference numbers, including a Reference Number given by the Office's CRM system, client reference numbers used by other agencies to identify the client may include details like the above for family members or other members of the public discussed by the complainant.

Retention of chat records will be stored to an individual profile, and are retained until our Organisation no longer has an account with the IVR platform. The contents of a Chat will be stored against the Profile of any User who is a participant in that Chat. The Chat data is not recorded against the call interaction it relates to. Agents will be given written instructions and refresher training on the appropriate use of the Chat function. The Office will monitor compliance by random audits and feedback as required.

These arrangements will be considered at the 12 month review.

Records are stored in accordance with the *Archives Act 1983* (Cth) and Records Authority of the Office of the Commonwealth Ombudsman 2008/00422945 – 30 September 2008. Relevantly, records are kept for 12 month, 5 year and 7 year timeframes depending on the type and complexity of the investigation, with some records retained for longer timeframes in accordance with archives legislation.

Will personal information be destroyed or de-identified once it is no longer needed for any authorised purpose? Do any of the exceptions apply (for example, the information is part of a Commonwealth record or the APP entity is required by law or a court/tribunal order to retain the information)?

Explain whether an exception applies that requires you to retain the information.

At such time as call recording is activated, the Office's ICT can set the parameters of storage and retention of call recordings. Call recordings will be stored in an encrypted manner and in compliance with the *Archives Act 1983* (Cth) and the relevant Ombudsman's Records Authority. Recordings relating to out of jurisdiction and lower complexity work may be retained on the IVR platform. Recordings relating to higher category approaches will be transferred to our complaints management system for retention.

These arrangements will be considered at the 12 month review.

If applicable, how will personal information be destroyed once it is no longer required?

Describe the method of destruction and explain how that method is secure.

⚠ **Privacy risk**: There is a risk of unauthorised disclosure if personal information is not securely and irretrievably destroyed.

If required by law or court order, the Office would contact QPC and third parties to effect destruction of records or information if it is no longer required. Otherwise, the information is securely stored in accord with archives timeframes.

If applicable, how will personal information be de-identified once it is no longer required?

Describe the method of de-identification that will be used and whether the de-identified information will be used for any other purpose. See the OAIC's De-identification and the Privacy Act for further information.

⚠ **Privacy risk**: If de-identifying personal information once it is no longer required, consider whether there is a risk that the information can be re-identified.

As above.

If you have outsourced personal information handling as part of this project, what will happen to information held by third party providers?

Describe any arrangements (for example, any contractual provisions) in relation to third parties' obligations to retain and dispose of personal information.

Privacy risk: If there are no arrangements in place relating to third parties' retention and disposal of personal information, there is a risk that personal information could be used by the third party for unauthorised purposes at the conclusion of the contract.

As above, the information is stored in the IVR Cloud platform in an encrypted manner and will not be accessed by third parties, apart from for utilisation to support the restoration of services should system failure occur.

APP 12 — Access to personal information

An APP entity that holds personal information about an individual must give the individual access to that information on request unless an exception applies.

How can individuals request access to their personal information? How will individuals be made aware of how to access their personal information?

Describe how individuals can request access, and who is responsible for handling such requests. If engaging third parties such as contracted service providers, consider whether there are arrangements in place to allow access to personal information held by third parties.

Individuals can ask to see their personal information held by us. If they think that it is wrong or not up to date and/or they can ask that it be corrected. It is anticipated that personal information stored on the IVR platform would constitute personal information and be subject to the Freedom of Information legislation as information held by contractors to a Commonwealth agency.

As per the Office's Privacy Policy:

> "If you are speaking to an Investigation Officer or a member the Public Contact Team you can ask them to immediately update information, such as your address or contact details if these have changed.
>
> More formal or extensive requests should be addressed to the 'Privacy Contact Officer' and sent via or email to ombudsman@ombudsman.gov.au. You can also call 1300 363 072 and ask to speak with a Privacy Contact Officer.

Generally, request for extensive changes to personal information will be considered with reference to the *Freedom of Information Act 1982* (Cth) (FOI Act) (for Commonwealth Ombudsman matters) and the *Freedom of Information Act 2016* (ACT) (for ACT Ombudsman matters). Individuals may also seek access to, or request amendment or annotation of, their personal information by submitting a request under relevant Commonwealth or ACT Freedom of Information Acts.

Are processes in place for responding to requests from individuals to access their personal information?

As per the Office's Privacy Policy:

> **"Access to personal information**
>
> If you receive a request under the Privacy Act for access to, or amendment of, personal information then this is usually decided by applying the principles that relate to the handling of requests for information made under the Freedom of Information Act 1982. See also APPs 12 and 13 above.

A person seeking access to personal information under the Privacy Act, APPs 12 and 13, specifically should be informed that if their request is dealt with as such then they will not be afforded the same review rights that flow from a decision under the relevant Freedom of Information Act/s. If a request is made under APP 12, the processes and procedures for accessing personal information will be followed.

If requests are made under the Commonwealth or ACT freedom of information legislation to amend or annotate records, for example to correct or annotate records that are caught by the QPC and IVR platform system, such requests will be actioned in accordance with legislative requirements.

APP 13 — Correction of personal information

An APP entity must take reasonable steps to correct personal information to ensure that, having regard to the purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading. The requirement to take reasonable steps applies in two circumstances: where an APP entity is satisfied that personal information it holds is incorrect, or at the request an individual to whom the personal information relates. There are minimum procedural requirements in relation to correcting personal information.

How can individuals seek correction of their personal information? How will individuals be made aware of how to correct their personal information?

Describe how individuals can seek correction of their personal information and how they will be made aware of this. If engaging third parties such as contracted service providers, consider whether there are arrangements in place to allow correction of personal information held by third parties.

This instruction is within the Office's Privacy Policy 2019, in the section titled 'How can I access or correct my personal information held by the Ombudsman?' (p. 11):

> "You can ask to see your personal information held by us. If you think that it is wrong or not up to date and/or you can ask that it be corrected. If you are speaking to an Investigation Officer or a member of the Public Contact Team you can ask them to immediately update information, such as your address or contact details if these have changed.
>
> More formal or extensive requests should be addressed to the 'Privacy Contact Officer' and sent via: land mail to GPO Box 442, Canberra ACT 2601; or email to ombudsman@ombudsman.gov.au.
>
> You can also call 1300 363 072 and ask to speak with a Privacy Contact Officer."

In the Privacy Policy 2019, in the section titled 'Voicemail records' (p. 18) states that:

> "Telephone calls to our main telephone number (1300 362 072) may be recorded when a telephone call is not taken (voicemail). These are registered on our phone system may relate to a range of matters, including complaints, general enquiries, media enquiries and contact by other agencies. The personal information contained in them may include a caller's name, address and telephone number. Depending on the subject matter of a recording the information contained in it will be placed onto other records will be reduced to a written form (not necessarily an exact transcription), and be handled accordingly. Some old records may have the audio recording filed. Once placed with the relevant record the recording (voicemail) is destroyed. These records may also be used for training and quality assurance purposes."

Individuals who contact the Office by phone (to be routed to authorised Agents through the IVR platform) will first hear the following recorded message:

> "The Ombudsman's Office may monitor or record your call for training and quality assurance purposes. Please inform the staff member you speak with if you do not wish for the call to be recorded.
>
> The Ombudsman's Office uses personal information we collect from you to assist us with our handling of your enquiry. Further information about the way the Ombudsman's office handles your personal information, including how you may access and seek correction of that information, can be found in the privacy statement available on our website ombudsman.gov.au
>
> The Office is working to improve our services may select you to provide feedback about your experiences. Please inform the staff member if you do not wish to participate."

Individuals can access a copy of the Privacy Policy 2019 from https://www.ombudsman.gov.au/about/privacy-policy and Privacy (ombudsman.gov.au)

As outlined above, individuals and persons have a right to request their personal information and records to be corrected or annotated if it is misleading or out of date under the *Privacy Act 1988* (Cth) and *Freedom of Information Act 1982* (Cth) and *Freedom of Information Act 2016* (ACT). Personal information that is relevant incomplete, incorrect, out of date or misleading can be corrected on application.

Are processes in place for responding to requests from individuals to correct personal information?

The Office's Privacy Policy 2019, in section titled 'How do I complain about the handling of my personal information by the Ombudsman' (pp. 12–13) explains that individuals are to send written complaints about privacy breaches or may call 1300 363 072 and ask to speak with a Privacy Contact Officer. This section then states:

> "… You should set out your reasons why you think we have not handled your personal information in accordance with the APP's. We will acknowledge your complaint within 7 days, investigate and attempt to resolve all complaints as soon as possible. Your complaint will be referred to a Privacy Contact Officer, usually a member of the Ombudsman legal team. Your complaint will be investigated and you will be advised of the outcome of the investigation. Our decision will be explained with reference to the relevant APPs. The time this will take will depend on the nature of your complaint and how complicated it is. If you are unhappy with our response or the way we have handled your complaint, you may make a complaint to the OAIC …"

As outlined above, individuals and persons have a right to request their personal information and records to be corrected or annotated if it is misleading or out of date under the *Privacy Act 1988* (Cth) and *Freedom of Information Act 1982* (Cth) and *Freedom of Information Act 2016* (ACT). Personal information that is relevant incomplete, incorrect, out of date or misleading can be corrected on application. The legislation provides for rights of review, including internal review and review by the relevant Information Commissioner or equivalent.

Are there process in place for associating a statement with personal information if a request for correction is denied?

Yes, there are processes and procedures in place under the *Freedom of Information Act 1982* (Cth) and ACT equivalent legislation and Privacy Act if an individual wishes to correct, annotate or amend their records. A person has a legal right to request this under the freedom of information legislation. A person or individual has the right to apply for internal review, lodge an application for external review by the Australian Information Commissioner or the ACT Ombudsman, or even to lodge a complaint about the process in accordance with the Office's Service Delivery Complaint Policy.

Are processes in place for identifying and correcting personal information that is inaccurate, out of date, incomplete, irrelevant or misleading?

Describe the steps that will be taken, or the measures that are in place, to ensure the ongoing integrity of the information.

Inbound calls routed to the Office through the IVR platform will be answered by authorised Agents. Upon receipt of the call, Agents will register the contact or complaint (including where the complainant requests to make the complaint anonymously) within the Office's CRM system. Agents will confirm with callers which phone number is to be recorded on the Office's CRM system.

As above, there are processes and procedures in place under the *Freedom of Information Act 1982* (Cth) and ACT equivalent and Privacy Act if an individual wishes to correct, annotate or amend their records.

Other considerations

Will any training be provided to staff to ensure the appropriate collection, handling and security of the personal information as part of this project?

Describe the type of training staff will receive.

No new training will be provided upfront – the information collected and handled is in line with what is currently collected and handled and staff have refresher on this training on an annual basis. Training on effective and appropriate use of IVR platform systems will be provided to staff who will be utilising the IVR platform system.

At a time when Call Recording is introduced, we would provide relevant training to staff on how to utilise call recording so as to ensure that this is completed in a secure and safe manner.

Does the project comply with your entity's other information handling or information management policies?

In its management of this project, the IVR Project Team seeks to comply with the Information Governance Framework which sets out the recordkeeping obligations and responsibilities of all staff; the Records and Information Management Naming Conventions; and the Email Management Policy.

Does the project recognise the risk of function creep? For example, is there an interest in using the personal information collected for the project for other purposes that might occur in the future?

No. The project is governed by the Head Agreement with the Digital Transformation Agency and short form contract with QPC.

Will this PIA be published?

Yes, on the Commonwealth Ombudsman's external website.

Are there any other broader privacy considerations associated with this project?

You might find it useful to show how the project will deal with other kinds of personal privacy not covered by the Privacy Act, such as bodily, behavioural and territorial privacy.

If you are an agency developing legislation or a new policy proposal with privacy impacts, consider whether any limitation on the right to privacy is reasonable, necessary and proportionate to your objective. For example, if you are developing legislation that seeks to rely on the required or authorised exception to the APPs (such as legislation authorising the use or disclosure of personal information), consider whether the proposed legislation is reasonable, necessary and proportionate to your objective. This may assist with the development of Human Rights Compatibility Statements for legislative projects.

Not applicable.

Privacy Management – Addressing Risks

A risk is something that could lead to the unauthorised collection, use, disclosure or access to personal information.

Use the table below to list each of the privacy risks identified and the mitigation strategies/tools that will be implemented to mitigate these. Add extra rows as required. Please specify the likelihood of the risk arising, the degree of impact it would have on individual's privacy if it occurred and an assessment (low/medium/high) of the residual risk. It may be helpful to categorise these risks into areas such as: governance, people, process, technology.

Risk Mitigation Table					
	Identified Risk	Mitigation Strategy	Likelihood	Impact	Risk Rating
1	Unauthorised access - staff, IVR Platform, QPC, other - leading to deliberate or accidental data release	No Direct Log-in will be enabled for QPC or the Office to access IVR Platform Cloud Office of the Commonwealth Ombudsman is responsible for authorising the addition of users to the '*GC CX 1 instance for the OCO*' and will do so through Microsoft Active Directory QPC User Access Management Standard – Information Security Management System Storage and Encryption will be as per the Telecommunications Marketplace Short Form Contract in place between the Office and Callscan Australia Pty Ltd.	Unlikely	Risk to individual safety/security if identifying or personal information is obtained Risk to reputation of the Ombudsman and the Commonwealth	Medium
2	Accidental data release through authorised access	Refresher training and feedback re conducting Proof of	Medium	Risk to individual safety/security if identifying or	High

		Record Ownership as set out in Our Complaint Handling Standard Operating Procedures. Reminders re Security, especially in regard to ensuring matching customer records and information being provided to the customer, whether verbally or in writing.		personal information is obtained Risk to reputation of the Ombudsman and the Commonwealth	

Recommendations

Summarise the recommendations to minimise the impact on privacy based on your risk assessment.

Ref	Recommendation	Agreed Y/N
R- 01	That the Office take reasonable and practical steps to ensure that QPC complies with its obligations under the contract with the Office to ensure the encryption, secure storage and transmission of data by QPC and its third party providers, including the IVR Platform provider, particularly so as to prevent unauthorised access and accidental access and disclosure of personal information, in accordance with the *Privacy Act 1988* (Cth), Australian Privacy Principle 11 and its contract with the Office. The Office will monitor compliance by random audits and feedback as required, Implement a review of the privacy impacts of the project in 12 months' time.	Y
R- 02	That the Office ensure that the cross-border flow of information is restricted and minimised to ensure so far as possible that data remains in Australia: Australian Privacy Principle 8. Where necessary to effect the IVR contract, information stored on the cloud will be stored securely. QPC will notify the Office of any eligible data breaches under the *Privacy Act 1988* (Cth) and cooperate with the Office to notify and remedy any potential breaches. The Office will monitor QPC's compliance with its legal and privacy obligations and the contract, including by random audits and consistent and clear channels of communication with QPC.	Y

Signatures

Lisa Collett

_____

Name of Senior Assistant Ombudsman responsible Signature

15/03/2023

Date

_____

Steven Mulipola, Privacy Delegate Signature

16/03/2023

Date