HM Revenue
& Customs

Conducting privacy impact assessments.

HMRC template (taken from the Code of Practice)

Step one: Identify the need for a PIA

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties. You may find it helpful to link to other relevant documents related to the project, for example a project proposal. Also summarise why the need for a PIA was identified (this can draw on your answers to the screening questions).

HMRC is deploying Voice Biometric technology (Voice ID) onto our telephony platform to complement our existing security processes, but provide the HMRC advisor with greater confidence that the customer they are purporting to be, is in fact them.

Customers will no longer have to answer the current ID&V questions every time they want to speak to HMRC as Voice ID will allow customers phoning specific LOBS to use their voice to confirm their identity once they have enrolled. Voice ID (enrolment and verification) will be available on the following LOBS.

In mid-January 2017, VoiceID was initially only available to Tax Credit (Classic ID&V TC - enrol only) and Self-Assessment customers, but will be rolled out to other lines of business. VoiceID (enrolment and verification) will be available on the following LOBS:

- PAYE
- ChB
- NI (customers only)
- Tax Credits (enrol and verification)
- DM-TC
- DM-SA

The benefits to the customer are –

1. Easier for the customer to 'pass' our security process
2. Reduce the waiting time for customers to speak to an advisor
3. Reduce the cost of the call
4. Increased confidence that their HMRC account(s) cannot be compromised

The benefits to HMRC are –

1. Increased confidence that we are speaking with the customer
2. Quicker to identify a fraudulent caller and deal with accordingly
3. Deterrence for potential fraudsters as they will not want to enrol their voice and may decide not target HMRC on the phones anymore
4. A reduction in the cost of transacting with the customer
5. Potential for Voice ID to be used multi-channel (digital) - should the business wish to pursue this
6. Prevention of fraud from entering HMRC systems and associated losses to the exchequer

The Project involves the use of personal data – the voiceprint. It was agreed in consultation with the Data Guardian, Project Team and CDIO stakeholders that a PIA is required.

The project will involve the collection of new information i.e.: the voiceprint. We will be using new technology that maybe perceived as being intrusive – the use of biometrics.

The PIA will be integrated within the project and we will include privacy issues alongside meetings, consultations and any other processes.

Step two: Describe the information flows

The collection, use and deletion of personal data should be described here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

HMRC Voice ID uses biometric technology to capture a voice sample from a live caller. This is compared to a previously stored voiceprint, which produces a confidence score of how closely the caller's voice sample matches the voiceprint.

A voiceprint includes more than 100 unique physical and behavioral characteristics of each individual, such as length of the vocal tract, nasal passage, pitch, accent, etc. Independent research has shown that a voiceprint is as unique to an individual as a fingerprint.

When a customer contacts us they will hear the usual welcome and introductions along with any broadcast message. Once ITA has determined what the customer has contacted us about, they are directed to the appropriate LOB. We ask the customer for their National Insurance number and they are presented with the ID&V questions for SA/ (eID&V for tax credits). If the customer passes security, they are then taken to the Enrolment module to register for HMRC Voice ID.

The customer is asked to repeat the phrase 'my voice is my password' up to five times - we need three utterances to capture a valid audio voiceprint, so the customer will have five chances to do this. Once completed they are queued ready to speak to the adviser when it is their turn.

This journey is all handled by ITA, but the functionality for an adviser to transfer the customer into the enrolment module will also exist using the CMA 'register' function.

HMRC will disclose the use of voice identification technology to our customers. Customers will also have the ability to opt-out, should they choose to.

Voiceprints are encrypted and stored in a secure database behind the firewall, just like any other sensitive customer data. The data stored, meets security standards. (**See Flow diagram** – CAF- on Vocal password process.) The audio files are stored in an IL3 environment encrypted with no customer identifiable data.

There is no delete function and KCom will hold the data for a number of years. (Work is currently ongoing regarding data retention)

HMRC is using Voice Identification (Voice ID) technology to help enhance the security of our customer's accounts, by reducing the risk of fraud and making information safer. The technology also makes it faster and easier for customers to speak to an HMRC adviser. It is more secure and will improve the customer journey.

Consultation requirements

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted, internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process. Consultation can be used at any stage of the PIA process.

The PIA will be integrated within the project and we will include privacy issues alongside existing meetings, consultations and any other processes.

We will work with the following stakeholders.

Internal:

- CS Change HOCS for PAYE, ChB, NI, DM-TC, DM-SA and TC
- NES
- KAI
- CS Change Process Owners
- CDIO Data Guardian
- Customer Service Data Guardian
- HMRC Communications and Marketing
- CDIO Communications and Marketing
- CDIO Digital Service

- Debt Management and Banking
- ITSC
- MDTP team
- DTUS

External

- BCCG representative groups
- KCOM
- Nuance
- User research (customers)

Step three: identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register. Annex three can be used to help identify the DPA related compliance risks Privacy issue Risk to individuals Compliance risk Associated organisation / corporate risk

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk
	If a retention period is not established information might be used for longer than necessary. The context is which information is used or disclosed can change over time, leading it to be used for different purposes. Measures/action taken against individuals as a result of collecting information could potentially seem to be intrusive.	Non Compliance with Human Rights legislation. Non Compliance with the DPA.	The use of biometric information may cause increased concern and cause people to avoid engaging with HMRC. Public distrust about we use the information could potentially damage HMRC’s reputation. Problems identified in the project may require a fix and a cost will be involved.

Step four: Identify privacy solutions Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Risk	Solution(s)	Result: is the risk eliminated, reduced, or accepted?	Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
1. Retention periods- If a retention period is not established information might be used for longer than necessary.	Devise retention periods which only keep information for as long as necessary.	Having a specific retention policy would reduce this risk – we would then need to establish how to enact it.	Yes - Having and implementing a policy would achieve this balance.
2. Storage- Anonymise the information	Information stored with encryption and no identifiable customer data.	Eliminated – the data stored in the Voice ID system would not enable individuals to be identified outside the system	Yes
3. Security process – enrol wrong person/Advisor not following security process	Implement security measures and standardised process. Produce Guidance for staff on how to carry out security process checks.	Reduced to within tolerance	Yes
4. Reputational damage to HMRC	• Ensure staff are properly trained and aware of new technology. Produce Guidance for staff on how to use the new system. • Ensure that individuals are aware how their information will be used. • Produce guidance and raise awareness on social media/press and promote with external bodies.	• Staff have been trained and provided with guidance. • A message about consent and data usage has been added when customers dial in. A specific privacy notice is in development. Further changes are under review. • The Voice ID system has been promoted to customers. We are currently seeking ways to increase transparency.	Once all these measures have been implemented, the balance will be achieved.

Step five: Sign off and record the PIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved solution	Approved by
1. Retention periods- If a retention period is not established information might be used for longer than necessary. 2. Storage- Anonymise the information 3. Security process – enrol wrong person/Advisor not following security process 4. Reputational damage to HMRC	1. Devise retention periods which only keep information for as long as necessary. 2. No further action. 3. No further action. 4. Develop privacy notice. Complete review of further changes.	1. Telephony Communication Service Team 2. N/A 3. N/A 4. Telephony Communication Service Team

Step six: Integrate the PIA outcomes back into the project plan

Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved?

Action to be taken?	Date for completion of actions	Responsibility for action
1. Devise retention periods which only keep information for as long as necessary. 2. Develop privacy notice. Complete review of further changes.	1. Devise retention periods which only keep information for as long as necessary. 2. Develop privacy notice. Complete review of further changes.	1. Telephony Communication Service Team working with SOLS and ODPO 2. Telephony Communication Service Team and Digital Operations Team, working with SOLS and ODPO

Who is the contact for any privacy concerns which may arise in the future contact point for future privacy concerns?

Head of Telephony Services, Telephony Communication Service Team

Date: 17/07/2018