Australian Government — Office of the Australian Information Commissioner

Threshold assessment template

August 2020

You are encouraged to take a flexible approach and adapt this template to suit your agency’s particular circumstances and internal processes. For example, you may wish to amend the project details section to capture the most relevant information for your agency or add additional factors to the table in Part 2 that point to the potential for your project to be a high privacy risk project based on your agency’s functions and activities.

## Project Details

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

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

|  |  |  |
| --- | --- | --- |
|  | Yes | Complete Part 2 of the assessment below. |
|  | No | It is not necessary to complete a PIA. Record the decision at Part 3 below and file this assessment with your privacy officer. |

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

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

| Will the project involve: | Yes | No |
| --- | --- | --- |
| **Handling large amounts of personal information?**  *Consider the amount of personal information and the number of individuals that will be impacted by your project.* *Even if you consider that each individual will only have a small chance of suffering a negative impact, handling personal information on a large scale can increase the privacy risk associated with your project. You should also consider whether your project will result in significant increases in the volume of personal information being handled through new or existing channels.* |  |  |
| **Handling sensitive information?**  *Sensitive information includes, but is not limited to, information about an individual’s racial or ethnic origin, political opinions, religious beliefs or affiliations, criminal records, sexual orientation or practices, biometric information[[1]](#footnote-1), health information and genetic information.*  *The privacy risk associated with your project can increase if sensitive information is involved given the potential for adverse consequences for an individual, or those associated with the individual, if it is mishandled (for example, discrimination, mistreatment, humiliation or embarrassment).* |  |  |
| **Sensitivities based on the context in which the project will operate?**  *Consider the context and circumstances surrounding the project. Are there prior concerns over this type of handling or activity? Is the project likely to have community support? Is the handling of personal information novel in any way? What is the current state of technology in this area and has there been any previously identified security or technology flaws? Are there any current issues of public concern that you should factor in? What is the nature of your relationship with individuals that may be impacted by the project? How much control will they have over the handling of their personal information? Would they expect you to use their personal information in this way?* |  |  |
| **Handling personal information of individuals with particular needs?**  *Consider whether the activity may have greater sensitivities or disproportionate impacts on certain populations or groups of individuals. This could include children and seniors, people with impaired intellectual or physical functioning, people who are not native speakers of the local language, people with low levels of literacy or education, people from a low socio-economic background, people experiencing financial hardship, people who are Aboriginal or Torres Strait Islanders.*  *An individual’s circumstances, or the increased power imbalance between the individual and an agency, may mean, for example, they are unable to easily consent to, or oppose, the handling of their personal information, understand its implications, or exercise control over their personal information.* |  |  |
| **Handling personal information in a way that could have a significant impact on the individuals concerned?**  *Consider the potential consequences for the individuals concerned. For example, negative impacts on physical and mental wellbeing, reduced access to public services, discrimination, financial loss or identity theft. Also consider whether the project has a significant collective impact on society, for example, increased surveillance and monitoring activities or the establishment of sensitive personal information sharing arrangements between the Commonwealth and other entities.* |  |  |

### Activity-based risk factors

| Will the project involve: | Yes | No |
| --- | --- | --- |
| **Using or disclosing personal information for secondary purposes?**  *A ‘secondary purpose’ is any purpose other than the primary purpose for which the APP entity collected the personal information.* |  |  |
| **Disclosing personal information outside of your agency?**  *Consider whether your project will involve sharing personal information with another agency, organisation or to any individuals other than the individual to whom the information relates. This might include the use of contractors or sub-contractors. Also consider whether your project will require the disclosure of personal information overseas or to an overseas-based company.* |  |  |
| **Using or disclosing personal information for profiling or behavioural predictions?**  *This includes valuation or scoring, profiling and predicting (including in relation to economic situation, health, personal preferences or interests, reliability or behaviour, location or movements).* |  |  |
| **Using personal information for automated decision-making?**  *This might include the use of artificial intelligence technologies or data analytics techniques on personal information to produce insights for policy-making or improved service delivery. It might also include using automated decision-making to make decisions that affect the rights, entitlements and opportunities of an individual.* |  |  |
| **Systematic monitoring or tracking of individuals?**  *For example, the introduction or enhancement of a surveillance system, the monitoring of communications, tracking an individual’s geolocation or behaviour.* |  |  |
| **Collecting personal information without notification to, or consent of, the individual?**  *This might include collecting personal information about an individual from a third party without the individual’s knowledge or consent. It might also include collecting personal information compulsorily under an existing, or proposed, legislative authority.* |  |  |
| **Data matching or data linkage?**  *For example, a new data matching program combining, comparing or matching personal information obtained from multiple sources or a data linkage[[2]](#footnote-2) project where information about the same person from different sources is brought together to create a unified dataset.* |  |  |
| **Developing legislation to modify the operation of one or more APPs or which seeks to rely on the required or authorised by law exception to the APPs?**  *This might include legislation or delegated legislation that seeks to modify the operation of one or more APPs in certain circumstances. It might also include legislation that seeks to rely on the required or authorised an exception to the APPs (such as legislation authorising the use or disclosure of personal information).* |  |  |

## Part 3: Decision & declaration

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

Based on your answers above, is a PIA required?

|  |  |  |  |
| --- | --- | --- | --- |
|  | Yes | Yes, a PIA is required.   |  | | --- | | *You may wish to include further detail or comments on the reasons why you have ticked one or more of the risk factors in Part 2 above.* | |
|  | No | No, a PIA is not required.   |  | | --- | | *Outline why it is not necessary to complete a PIA. This may be because the project does not involve personal information (for example, de-identified data is being used) or the project does not involve a new or changed way of handling personal information (refer to your assessment at Part 1 above). If the project is not new, you could include a description of how privacy risks have previously been assessed and are being managed*.  *If you have ticked one of the boxes in Part 2 above, but have determined that a PIA is not necessary, outline your reasons why. It is the responsibility of each agency to be able to justify why a new or changed way of handling personal information does not have the potential to be high privacy risk.* | |

|  |  |  |  |
| --- | --- | --- | --- |
| Assessor Sign-off | | | |
| Name |  | Position | Date |
|  | |  |  |
| Approver Sign-off | | | |
| Name |  | Position | Date |
|  | |  |  |
| Privacy Officer Sign-off | | | |
| Name | | | Date |
|  | | |  |

1. Biometric information is an electronic copy of an individual’s face, fingerprints, iris, palm, signature or voice. [↑](#footnote-ref-1)
2. Data linkage may also be referred to as ‘data integration’. [↑](#footnote-ref-2)