# **Privacy Impact Assessment (PIA) Template**

**Project overview**

Identify the need for a Privacy Impact Assessment (PIA)

A Privacy Impact Assessment assists organizations in identifying and managing data privacy risks associated with any new activity, such as new programs, technology, or policies. For more details on when a PIA is needed, and general PIA questions, please see the PIA Guidance document in this folder. If you have questions about some of the terms used here, review the Responsible Data Definitions document in the Definitions folder.

Explain what this project or technology aims to achieve, and what the benefits will be to the organization, to individuals and other parties.

|  |
| --- |
|  |

Questions to consider, as you determine the need for a PIA:

* Does this involve the collection of information about individuals?
* Will this activity or program compel individuals to provide information about themselves?
* Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
* Does this involve using new technology (e.g., biometrics) which may be perceived as being privacy intrusive?
* Will this activity or program result in you making decisions or taking action against individuals in ways which can have a significant impact on them?
* For the data you will collect, are the information types (e.g., health records, refugee status) likely to raise privacy concerns or expectations?

If the answer to any of these questions is yes, a PIA is required.

Privacy Impact Assessment plan

Describe the parameters for this PIA.

|  |
| --- |
| * Team (PIA conductors, key stakeholders) * Timeline * Legal considerations * Program considerations (if relevant) * Expected level of effort and complexity |

**Data Analysis**

Data Types

Identify the types of data that will be involved in this project or technology. If you will be collecting the data types mentioned below, please provide examples in the comments column.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Type** | **Yes** | **No** | **Don’t know** | **N/A** | **Comments** |
| Will you use (e.g. collect, store, transmit, analyze etc.) personal data that directly identifies individuals? |  |  |  |  |  |
| Will you use data that does not directly identify an individual, but that could be used to single out an individual by applying existing and readily accessible means and technologies? |  |  |  |  |  |
| Will you use sensitive data? |  |  |  |  |  |

Data Access and Use

Identify how data will be collected, accessed and used

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Direct from individual** | **Data provider** | **Don’t know** | **Comments** |
| How will the data be obtained? |  |  |  |  |
| **Type** | **Yes** | **No** | **Don’t know** | **Comments** |
| Do you have a legitimate interest for your data access and use? |  |  |  |  |
| If obtaining data from a provider, do they have a legitimate interest to provide access to the data for the purpose of the project? |  |  |  |  |
| Have you defined your data use purpose as narrowly and practically as possible? |  |  |  |  |
| Are you minimizing the amount of data collection that will be necessary? |  |  |  |  |
| Is the purpose for which you will be **using** the data compatible with the purpose for which you **obtained** the data? |  |  |  |  |
| Are all the data that you will be using stored for no longer than the time necessary, for the specified purposes? |  |  |  |  |
| Is your data accurate, up to date and relevant to the purpose of the project? |  |  |  |  |
| In order to protect your data from a breach or data incident, have you employed appropriate and reasonable technical and administrative safeguards, such as strong security procedures, vulnerability assessments, or de-identification? |  |  |  |  |
| Are your partners, data providers or technologies compliant with, at a minimum, Mercy Corps’ data privacy and data protection standards and principles, as outlined in this checklist? |  |  |  |  |
| Is your use of the data compliant with a) applicable laws and policies, and b) the terms under which you obtained the data? |  |  |  |  |
| Have or will you communicate out about the data use or other related information? If so, who will you communicate with (the data subject, public, or others) and will the data comms be at an aggregate or individual level? |  |  |  |  |

Another option is to consider creating a map of information flows relevant to this PIA: what information will be collected, used and disclosed, how it will be held and protected, and who will have access to it.

Questions to ask when creating an information flow map:

* How will the data be collected (e.g., print, online, mobile device)?
* Are there any limits on the nature of the data to be collected (e.g., age, gender)?
* Is it necessary to collect personal data from individuals, or can we collect information anonymously or pseudonymously? Can individuals choose not to provide some or all the personal information?
* How will an individual’s circumstances be considered when the personal data is being collected?
* What type of data collection notice will be given to the individual, and how will it be given? For example: purpose, use, disclosure, and legal implications, and choices around the use of that data.
* How often will the personal data be collected?
* How will data be shared or transferred?
* What options does the individual have, if their data needs to be accessed, updated or deleted?

Data Risks

Identify the types of potential data risks for this project or technology. For the risk mitigation column, indicate yes or no. The next section will address the risk mitigation details.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Type** | **Yes** | **No** | **Don’t know** | **N/A** | **Comments/Risk mitigation** |
| **Individual** | | | | | |
| Are there any risks or harms associated with the publication of the collected data or resulting reports, and are the risks extremely high compared to the benefits? |  |  |  |  |  |
| What types of information, if any, will be de-identified? |  |  |  |  |  |
| Will any potentially sensitive or intrusive methods of collection be used? (e.g., photographs, biometrics, signatures)? |  |  |  |  |  |
| Does your project, technology or use of data pose any risks of harm to individuals or groups of individuals, whether or not they can be directly identified, visible or known? |  |  |  |  |  |
| **Type** | **Comments** | | | | |
| **Compliance** | | | | | |
| If you are relying on consent to process personal data, how will this be collected and what will you do if consent is withheld or withdrawn? |  | | | | |
| How are you ensuring that personal data obtained from individuals or other organizations is accurate? |  | | | | |
| What retention periods are suitable for the personal data you will be processing? |  | | | | |
| What mechanism or tool will be used to handle complaints? Is the tool visible, comprehensive and effective? |  | | | | |
| What audit, oversight measures and technical safeguards are in place in case a system or process fails? |  | | | | |
| **Type** | **Yes** | **No** | **Don’t know** | **N/A** | **Comments/Risk mitigation** |
| **Security** | | | | | |
| Do the proposed new systems provide protection against the security risks you have identified? |  |  |  |  |  |
| Do you have necessary training and instructions to ensure that team members know how to operate any new systems securely? |  |  |  |  |  |
| Will the systems you are putting in place allow you to respond to subject access requests more easily? |  |  |  |  |  |
| Will the systems be able to prevent and detect data misuse or inappropriate access? |  |  |  |  |  |
| If the data will be shared with external parties, is there a data sharing agreement (DSA) in place? |  |  |  |  |  |
| **Access** | **Comments** | | | | |
| How will you handle data or privacy? |  | | | | |
| How valuable would the information be to unauthorized users? |  | | | | |
| Which internal groups or teams will have access to the data? |  | | | | |
| Which external parties will have access to the data, such as vendors, implementing partners or other NGOs? |  | | | | |

**Risk Analysis**

Risk Mitigation

Identify all the risks noted above (Individual, Compliance, Security, Access) where you have answered Yes, or entered concerns in the Comments or Risk Mitigation columns. In the table below, please enter each of the identified risks, then describe how you will mitigate or resolve these risks.

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk** | **Solution** | **Result** | **Evaluation** |
| EXAMPLE: Do you have necessary training and instructions to ensure  that staff know how to  operate a new system  securely? | Detailed training is easily provided. | Trained staff | Acceptable |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Mitigation Outcomes

For each mitigation option identified above, describe next steps.

|  |  |  |
| --- | --- | --- |
| **Action to be taken** | **Due date** | **Responsible party** |
| EXAMPLE: Staff trained on handling of each request type | Within 30 days of launch | Program Manager |
|  |  |  |
|  |  |  |
|  |  |  |

**Final assessment and recommendations**

After reviewing the above and reflecting on your answers, how will you proceed?

* The risks and harms are not likely, and if they are, they would not be severe. Moreover, the benefits outweigh these risks. I will proceed with the project.
* The risks and harms are more severe than the potential benefit of the project. However, I can mitigate the risks and proceed with the project.
* The risks and harms are more severe than the potential benefit of the project.
* The risks cannot be mitigated. I will cancel the project.
* I do not know. I need more guidance from domain and data experts (legal, privacy, security, etc.).

|  |
| --- |
| Additional comments |

|  |
| --- |
| Signatures from core PIA team |