**PIA for a New Policy**

1. Explain the purpose/goals and expected benefits for your activity, both inside and outside Mercy Corps. Please provide as much detail as possible.
   1. Purpose/goals:
   2. Expected benefits:
2. Provide the following activity details
   1. Team
      1. Main contact:
      2. Key stakeholders:
   2. Timelines:
   3. Special considerations that could impact your activity:
      1. Legal (compliance with local, national or industry regulations):
      2. Country/Security (country risk level, local security concerns):
      3. Other:
   4. Expected level of effort and complexity:
   5. If relevant, GAIT ID/link:
3. Is your activity subject to particular donor or program requirements, project needs, or the European Union’s General Data Protection Regulation (GDPR)?
   * If yes, list those requirements here:
   * If no, skip to question 4.
   * If you don’t know, then please check with your supervisor, program lead or whoever is responsible for understanding legal/donor requirements for your activity.
4. Please select the option below that best represents your new activity
   * [Policy](#kix.aj69ba37gyje)
   * [Process or procedure](#kix.aecshxs0ihaj)
   * [Software or technology system](#kix.13ldjr7vyzjd) **only**
     + This is primarily meant for implementation of new global, country-wide or team-specific systems.
     + If you are selecting or using a new system as part of a larger project or program, *use the* [*project or program*](#kix.o9o0ylf3114) *option instead.*
   * [Vendor or partner](#kix.vqo87cr9wc5j) **only**
     + This is primarily meant for validation of a vendor, partner, or third party’s activities as part of a unique or one-time activity.
     + If you are selecting or using a new vendor, partner or third party as part of a larger project or program, *use the* [*project or program*](#kix.o9o0ylf3114) *option instead*.
   * [Project or program](#kix.o9o0ylf3114)
     + This can be for any phase or aspect of a project or program.
     + *This is the most comprehensive PIA option*, and includes language for also selecting new software or tech systems, and/or a new vendor or partner.

**Note:** if your activity involves multiple elements - for example, a new policy that involves a new procedure and new software - then fill out each section below as needed. There is no need for multiple PIAs to be completed, when they all can be combined into one.

**Policy: Data Details**

Data Fundamentals

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Data types** | **Yes** | **No** | **Don’t know** | **Details** |
| Will your policy address the use of de-identified or anonymized data? That is, the data will not directly identify an individual, but could be used to identify them by applying existing and readily accessible data or tools?  If yes, please also address this risk in the Risk Mitigation section. |  |  |  |  |
| Will your policy address the use of sensitive data? That is, the personal data is of a nature that could be used to target an individual? |  |  |  |  |

|  |  |
| --- | --- |
| **What personal or sensitive data fields will be addressed in this policy?** | |
| Personal: |  |
| Sensitive: |  |

**Note:** if your policy will address the use of sensitive data, you must also review the [Sensitive Data Guidance](https://library.mercycorps.org/record/38516) to ensure proper policy statements around the use of this data.

Data Collection

|  |  |
| --- | --- |
| **Will data collection be addressed in this policy?** Please provide details. | |
| Yes - Direct from individual(s) |  |
| Yes - Third party (government, NGO, vendor, partner, etc) |  |
| No- not applicable | If no, skip to next section: **Data Purpose and Scope** |

|  |  |
| --- | --- |
| **Will this policy address the formats (paper, digital) and locations (software/technologies, work or personal devices) will this data be collected, managed, or stored?** Please provide details, particularly if the technologies used are not in the [MEL Tech Suite](https://library.mercycorps.org/record/37835?ln=en) or a standard enterprise application. | |
| Collected |  |
| Managed |  |
| Stored |  |

|  |
| --- |
| **Will this policy address potentially more invasive methods of data collection? (e.g., taking photographs, using biometrics, collecting signatures)?** If yes, please also address this risk in the Risk Mitigation section. |
|  |

|  |
| --- |
| **Will this policy address the frequency of data collection?** |
|  |

|  |
| --- |
| **How will an individual’s circumstances be considered when the personal data is being collected as part of this policy?** |
|  |

|  |
| --- |
| **What type of data collection notice will be given to the individual, and how will it be given as part of this policy?**  For example: purpose, use, disclosure, and legal implications, and choices around the use of that data. |
|  |

Data Purpose and Scope

Every personal data-related activity must have a lawful basis for the processing of that data.

|  |  |
| --- | --- |
| **As part of this policy, what lawful basis are you using to collect or process this data?** [**Go here**](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/#what) for more information on lawful bases, but please select one or more legal bases noted below, then provide details on why that basis applies to your activity. | |
| **Consent**: the individual has given clear consent for you to process their personal data for a specific purpose. |  |
| **Contract**: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract. |  |
| **Legal obligation**: the processing is necessary for you to comply with the law (not including contractual obligations). |  |
| **Vital interests:** the processing is necessary to protect someone’s life. |  |
| **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law. |  |
| **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests. |  |

|  |
| --- |
| **If this policy will rely on consent to process personal data, how will consent be collected, and what will you do if consent is withheld or withdrawn?**  If already available, please note the specific language to be used, or link to an existing template.If yes, please also address this risk in the Risk Mitigation section. |
|  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Scope** | **Yes** | **No** | **Don’t know** | **Details** |
| If the policy addresses obtaining data from a third party, do they have a legitimate interest for the data access and use? |  |  |  |  |
| Have you narrowed the purpose of this policy so as to [minimize the amount of data collection](https://library.mercycorps.org/search?ln=en&as=1&m1=a&p1=Responsible+Data%3A+Definitions&f1=title&op1=a&m2=a&p2=&f2=&op2=a&m3=a&p3=&f3=&dt=&d1d=&d1m=&d1y=&d2d=&d2m=&d2y=&rm=&ln=en&action_search=Search&sf=&so=d&rg=25&fti=0&fti=0) that is necessary? |  |  |  |  |
| Will this policy ensure data is used for the same purpose for which the data was obtained? |  |  |  |  |
| Could implementation of this policy cause harm, or risks of harm to individuals or groups, whether or not those harms can be directly identified or visible?  If yes, please also address this risk in the Risk Mitigation section. |  |  |  |  |

Data Accuracy, Retention and Use

|  |
| --- |
| **Who will have access to the data as part of this policy? This is both inside and outside of Mercy Corps** Please also address this risk in the Risk Mitigation section. |
|  |

|  |  |
| --- | --- |
| **If this policy addresses data obtained from or shared with a third party:** | |
| Is there a data sharing agreement (DSA) in place?  Please also address this risk in the Risk Mitigation section. |  |
| Will the third party share this data with any other third parties, whether that is another partner, sub-contractor, or technology/service?  If yes, please also address this risk in the Risk Mitigation section. |  |

|  |  |
| --- | --- |
| **Will this policy address the formats (paper, digital) and locations (software/technologies, work or personal devices) will this data be collected, managed, or stored?** Please provide details, particularly if the technologies used are not in the [MEL Tech Suite](https://library.mercycorps.org/record/37835?ln=en) or a standard enterprise application. | |
| Collected |  |
| Managed |  |
| Stored |  |

|  |
| --- |
| **How will this policy ensure the initial and ongoing accuracy of the data?**  Please also address this risk in the Risk Mitigation section. |
|  |

|  |
| --- |
| **Explain how this policy will allow an individual to request access, updates to or deletions of their data.** |
|  |

|  |
| --- |
| **How will this policy ensure the data will be stored no longer than is necessary? What retention periods are suitable for the personal data you will be processing?**  Please also address this risk in the Risk Mitigation section. |
|  |

|  |
| --- |
| **What mechanism or tool will be used to handle complaints for implementation of this policy? Is the tool visible, comprehensive and effective?**  Please also address this risk in the Risk Mitigation section. |
|  |

|  |
| --- |
| **Will the policy you are putting in place allow you to easily understand what data is held on an individual and report on that data if necessary?** If yes, please also address this risk in the Risk Mitigation section. |
|  |

|  |
| --- |
| **Will the policy address activity reports, and if so, what type of reports and who will reports be shared with?** |
|  |

Data Security

For this section, you will need to have a firm understanding of the systems and tools being used as part of your activity. If you have any questions about how to answer these questions, please contact your local IT admin, or the Data Protection and Privacy team.

|  |
| --- |
| **For the systems being used as part of this policy, do you have the necessary training and instructions to ensure that team members know how to operate these systems securely?** Please also address this risk in the Risk Mitigation section. |
|  |

|  |
| --- |
| **Will the above systems be able to prevent and detect data misuse or inappropriate access in relation to this policy?** Please also address this risk in the Risk Mitigation section. |
|  |

|  |
| --- |
| **If relevant, does your policy ensure that any relevant partners, data providers or systems, and their data use, are compliant with Mercy Corps’** [**Responsible Data Policy**](https://library.mercycorps.org/record/30303?ln=en) **and applicable laws and policies?**  The best way to document this requirement is to link to or refer to existing security, privacy, or contract-related materials from your partner, data provider, or system/technology provider. The key is to provide materials that clearly show that the third party is complying with global and industry standards. |
|  |

|  |
| --- |
| **What audit, technical and administrative safeguards will this policy address, to avoid the possibility of a data breach or incident?**  Please also address this risk in the Risk Mitigation section. |
|  |

|  |
| --- |
| **What steps will this policy outline for handling a suspected data or privacy breach?** Please provide details including main point of contact, local and global response. |
|  |

**Risk Analysis**  
Risk Mitigation

Several questions above include this statement: Please also address this risk in the Risk Mitigation section. For each risk-related question you answered, discuss that risk in the table below, then describe how you will mitigate or resolve these risks.

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk** | **Solution** | **Outcome** | **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, including Data Protection and Privacy team and/or MEL/KM team review:  Assessment completion dates:   * Pre-activity: * Activity start: * Final (1 year from activity start): |