# **Privacy Impact Assessment: Podio**

**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.

|  |
| --- |
| The Responsible Data Program needs a global tool that allows for secure submission and tracking of requests related to data protection and privacy. The tool can be used to request responsible data guidance, document review (such as PIAs, data sharing agreements), and subject access requests including data removal. By using a single tool across the agency, we can ensure consistency and accuracy across requests, increase knowledge of best practices, and examine trends for future learning opportunities.  The tool under consideration is [Podio](https://podio.com/), and a dedicated workspace for Responsible Data requests already exists here: <https://podio.com/mercycorps/data-protection-privacy> |

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 owner: Heather Love   + Key stakeholders: Steven Cox, Kayleigh Logan-Cleghorn, Alexandra Angulo, Marina Antunovic * Timeline: May 2020 * Legal considerations: Tool will be managed by staff in the United States, UK and EU. As a result, the tool and its usage must comply with relevant law in these locations, as well as Mercy Corps’ Responsible Data Policy. * Program considerations: n/a * Expected level of effort and complexity: Moderate |

**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? | X |  |  |  | In order to respond to requests, some amount of personal data must be collected. |
| 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? |  | X |  |  | Since the purpose of this tool is to respond to individuals directly, there is no reason to disaggregate. |
| Will you use sensitive data? |  | X |  |  | The likelihood of sensitive data being collected or provided is extremely unlikely. |

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? | X | X |  | Individuals will submit their information/data via email or through a Podio form. This will be the primary way data is collected.  A data provider would be an external company, such as SayMine. Information from data providers will be provided rarely, and only when the individual chooses to use that provider. |
| **Type** | **Yes** | **No** | **Don’t know** | **Comments** |
| Do you have a legitimate interest for your data access and use? | X |  |  |  |
| If obtaining data from a provider, do they have a legitimate interest to provide access to the data for the purpose of the project? |  |  | X | Case by case evaluation is required. For [SayMine](https://saymine.com/faq), the answer is yes, they have a legitimate basis. |
| Have you defined your data use purpose as narrowly and practically as possible? | X |  |  |  |
| Are you minimizing the amount of data collection that will be necessary? | X |  |  | Initial requests only require an individual to enter their name and email address. Additional information is volunteered at their direction. Subject access requests may require additional information from the individual, in order to do research and locate their data in Mercy Corps systems. |
| Is the purpose for which you will be **using** the data compatible with the purpose for which you **obtained** the data? | X |  |  | The information will only be used to complete each request. |
| Are all the data that you will be using stored for no longer than the time necessary, for the specified purposes? | X |  |  | Data will be retained for a minimum of seven years, longer if required per program, country or legal needs. |
| Is your data accurate, up to date and relevant to the purpose of the project? | X |  |  | Data is accurate at the time of initial request; there is no need to keep the information updated once the request is complete. |
| 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? | X |  |  | Read/edit access to the Podio workspace is limited only to those who manage a request, or are part of the Responsible Data Program.  Also see [Podio security standards](https://help.podio.com/hc/en-us/articles/201018968-Podio-Security). |
| 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? | X |  |  | See [Podio data protection standards](https://help.podio.com/hc/en-us/articles/360000980392-Where-is-data-hosted-). |
| Is your use of the data compliant with a) applicable laws and policies, and b) the terms under which you obtained the data? | X |  |  | As per above, all relevant standards will be addressed and met. |
| 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? | X |  |  | Communication to the individual is required in order to complete their request.  Research with other Mercy Corps teams will be required in order to complete some requests. We will only share enough data to sufficiently complete those requests. |

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? |  |  |  | X | No plans to share data |
| What types of information, if any, will be de-identified? |  |  |  | X | Only using data provided by the individual, which will be minimal and required in order to complete the request.. |
| Will any potentially sensitive or intrusive methods of collection be used? (e.g., photographs, biometrics, signatures)? |  | X |  |  |  |
| 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? | X |  |  |  | True for any PII collection, but only using the data to complete the individual’s request. |
| **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? | Individual will only submit request so that we can process their request | | | | |
| How are you ensuring that personal data obtained from individuals or other organizations is accurate? | Only using data submitted by the individual | | | | |
| What retention periods are suitable for the personal data you will be processing? | Data will be retained for a minimum of seven years, longer if required per program, country or legal needs. | | | | |
| What mechanism or tool will be used to handle complaints? Is the tool visible, comprehensive and effective? | Podio request form is available to all MC team members. Complaints can be escalated to the MCG CIO or MCE Executive Director. | | | | |
| What audit, oversight measures and technical safeguards are in place in case a system or process fails? | See [Podio security standards](https://help.podio.com/hc/en-us/articles/201018968-Podio-Security). In addition, access is limited to the reviewers of this document, and MCG CIO. | | | | |
| **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? |  | X |  |  | Existing Podio technology and MC practices provide sufficient protection |
| Do you have necessary training and instructions to ensure that team members know how to operate any new systems securely? | X |  |  |  | Easily provided |
| Will the systems you are putting in place allow you to respond to subject access requests more easily? | X |  |  |  |  |
| Will the systems be able to prevent and detect data misuse or inappropriate access? | X |  |  |  | Internal access will be limited to necessary staff, which limits risk of data misuse. |
| If the data will be shared with external parties, is there a data sharing agreement (DSA) in place? |  |  |  | X |  |
| **Access** | **Comments** | | | | |
| How will you handle data or privacy breaches? | Podio will notify Mercy Corps if there is a data center breach. Internally, we would be responsible for alerting requesters about the breach, in alignment with our Incident Response Plan. | | | | |
| How valuable would the information be to unauthorized users? | Very little, since the data’s purpose is to fulfill a compliance-related request | | | | |
| Which internal groups or teams will have access to the data? | Read/edit access to the Podio workspace is limited only to those who manage a request, or are part of the Responsible Data Program/leadership. As of May 2020, that is 6 staff. | | | | |
| Which external parties will have access to the data, such as vendors, implementing partners or other NGOs? | None | | | | |

**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** |
| 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? | True for any PII collection, but only using the data to complete the individual’s request. Extremely low risk. Also, internal access will be limited to necessary staff. | Limited data use, limited access. | Acceptable |
| Do you have necessary training and instructions to ensure that team members know how to operate any new systems securely? | Training is easily provided. | Trained staff | Acceptable |
| Will the systems you are putting in place allow you to respond to subject access requests more easily? | SAR requests will initially come via email, and then the Podio workspace will be used to manage the details. | New procedures will be created. | Acceptable |
| Will the systems be able to prevent and detect data misuse or inappropriate access? | Internal access will be limited to necessary staff. Data changes result in email notification, so ensure staff notifications are on. | Email notifications capture changes -- unwanted changes will be easily noted. | Acceptable |

Mitigation Outcomes

For each mitigation option identified above, describe next steps.

|  |  |  |
| --- | --- | --- |
| **Action to be taken** | **Due date** | **Responsible party** |
| Staff trained on Podio | July 2020 | Heather Love |
| Staff trained on handling of each request type | July 2020 | Heather Love |
| Staff trained on creating Podio email notices | July 2020 | Heather Love |
|  |  |  |

**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 |