TIP SHEET 1

PRIVACY IMPACT ASSESSMENT (PIA)

elan
The Electronic Cash Transfer Learning Action Network

WHAT IS A PRIVACY IMPACT ASSESSMENT (PIA)?

A Privacy Impact Assessment (PIA) is a systematic analysis of the potential privacy risks related to data collected during program implementation. A PIA analyzes threats and risks to program data, including any legal and environmental factors, and develops mitigation strategies. PIAs help humanitarians protect participants' privacy and strengthen public confidence in the program.

WHAT HUMANITARIANS NEED TO KNOW:

A PIA should be conducted before data collection starts - usually during a program's planning or inception phase – so that any potential problems can be proactively addressed. Alongside identifying privacy risks, the PIA exercise can be useful in raising overall data privacy concerns between the implementing organization(s), partners, and program participants.

All PIAs should take contextual elements into account; as such, risk assessments may look very different in different country contexts, even if programs themselves are similar. Depending on the sensitivity of the data your program will be collecting, you may want to consider working with an external privacy assessment specialist.

As stated in the Cash Learning Partnership (CaLP) *Protecting Beneficiary Privacy: Principles and Operational Standards for the secure use of personal data in cash and e-transfer programs (page 11)*

- *Identify the privacy risks to individuals*
- *Identify the privacy and data protection compliance liabilities for the organization*
- *Protect the organization's reputation and instill public confidence in the program*
- *Ensure that the organization is promoting human rights in its humanitarian activities*

WHAT HUMANITARIANS CAN DO:

SELECT OR ADAPT PIA GUIDANCE

The following steps are adapted from *suggested guidance* from the Privacy Commissioner of New Zealand; please adapt them to fit your individual organization. You may also find CaLP's *Model Privacy Impact Assessment* helpful (pages 19-20). For more detailed guidance, please refer to the "Additional Resources" section at the end of this Tip Sheet.

Step 1: Review your program

Describe your program objectives and activities and outline the different types of data that will be collected, as well as the rationale for collecting this data. Specifically note where personally identifiable information (PII) is collected and used throughout the program since many risks relate to this data (see step 3). Within this list, indicate which data will be collected directly by your organization and which data will be collected by a partner (e.g., participants' transactions records held by a financial service provider). Include details about how and with whom program data will be shared and/or published. Include the cultural context in the description, if relevant.

Draw an information or data lifecycle to highlight the individual data steps, indicating what will happen at each step, who is involved, and how information is transferred between users or organizations.

Step 2: Educate yourself about relevant privacy regulations

Be sure to understand which regulations apply to the data you will be collecting and compare your planned programmatic steps against the legally-established privacy principles of the relevant jurisdiction(s). *(See Know Your Customer—KYC—Tip Sheet.)* Be aware that you might need to take into account multiple regulations (e.g., the location where data is collected, where the data is sent, and/or the legal home of relevant organization(s) or partner(s), as well as donor regulations). In addition to national regulations like KYC, regional or international agreements may also apply.

Alongside legal privacy regulations, include your organization's privacy principles and ethical guidelines in your analysis. If your organization has not developed these, use CaLP's as a starting point. After completing this process for your first e-transfer program, it will become easier to check for updates and adapt this review process for future programs.

Step 3: Identify any privacy risks

Compare the steps you outlined in the data lifecycle (Step 1) against any relevant privacy regulations (Step 2). Based upon regulatory guidelines, are there any differences between how you plan to manage data and how you should be managing data? Think carefully about who might try to improperly use each type of data, how they could gain access, and what would happen if they were successful.

Step 4: Evaluate and mitigate risks

Using the list you established in Step 3, prioritize which are the biggest risks to your data and their likelihood of occurrence. Keep in mind that low-likelihood risks that are potentially damaging should not necessarily be de-prioritized. Use this analysis to identify particular weaknesses in your program plans that need to be addressed. Then, identify mitigation strategies in response to those risks. As you develop mitigation strategies, make sure to include all of the people involved in these different program stages (i.e., field and M&E officers, finance team members) to ensure feasibility of the strategies you develop.

Example risk: An e-transfer service provider enables your NGO to restrict access to PII within the backend platform. However, if the PII contained in the system is exported to an Excel spreadsheet and saved on a shared drive, these restrictions no longer apply, since all staff now have access to the data.

Example mitigation strategy: Restrict the permissions to export data and include guidance in Standard Operating Procedures (SOPs) on securely storing exported information.

Step 5: Draft an accessible PIA report

Clearly document the risks, potential impacts and mitigation actions in your PIA report, since program staff will refer back to this document throughout program implementation. Be explicit about how often this report should be consulted, and whether a formal review of the PIA should be conducted during the program. There is not standard guidance about how often a PIA should be reviewed, but a good rule of thumb is to conduct a review on an annual basis.

Draft the PIA report using simple, accessible language so it can be easily understood by all staff and include definitions of any technical terms *(or link to the Starter Kit Glossary)*. If your PIA is particularly long, consider drafting a short Executive Summary to highlight the main decisions that were made based on the assessment. Also, think about how you can structure or present the information in an easily-digestible format (e.g., matrix, data lifecycle diagram) and any needs for translation into a local language.

Step 6: Make an action list

Based on your PIA report or summary, develop a list of concrete tasks and conditions that are required for the PIA to be effective. For example, identify who needs to be made aware of the report, which new tools need to be substituted for less secure ones, what revisions to program plans or SOPs are required. Build the risk-mitigation measures identified in the PIA into your SOPs, and periodically review the effectiveness of these measures.

Step 7: Compare PIAs at the end of similar programs

If similar risks are present in multiple PIAs, it might be a sign that new policies need to be adopted at a higher level to address these risks. Assign a person or a team to cull through PIAs to identify commonalities to inform country or organizational practices.

GET THE MOST OUT OF YOUR PIA

Keep track of your formats and be ready to adapt based on your assessment findings

The most important data sets in e-transfer programs are those that contain program participants' PII. Your organization may hold parts of this data in different formats. When you identify these sensitive data sets and mitigation strategies through your PIA, make sure to apply these strategies to all versions or portions of the sensitive data set.

Adapt based upon your findings

Thinking through your risks and their likelihood (also known as your threat model) may highlight some gaps in your program design. You may need to hire specialists to assist with developing mitigation strategies for these threats or adjust your program plans to respond to identified gaps.

ADDITIONAL RESOURCES:

Privacy by Design. UK Information Commissioner's Office. A component of its overall guide to data protection, this section includes an explanation of privacy by design, the importance of PIAs, and a *code of practice for carrying out a Privacy Impact Assessment.*

Model Privacy Impact Assessment. *Protecting Beneficiary Privacy: Principles and Operational Standards for the Secure Use of Personal Data in Cash and E-transfer Programs*. CaLP. Annex 1, pp. 19-20.

Privacy Impact Assessments. US Government Federal Trade Commission (FTC). A list of publicly-available PIAs drafted for different programs and projects of the FTC. The text itself is not particularly relevant for the cash transfer world, but the assessments are good examples of sector-specific PIAs.

Privacy Impact Assessment Toolkit. Privacy Commissioner's Office in New Zealand. Templates and checklists to help construct a PIA and choose which elements to include.

McDonald, Sean. *Ebola: A Big Data Disaster: Privacy, Property and the Law of Disaster Experimentation*. CIS Papers. January 2016. A general piece about the complexity of potential legal risks and liabilities when humanitarian organizations capture PII.

The Electronic Cash Transfer Learning Action Network is convened by Mercy Corps, with support from the MasterCard Center for Inclusive Growth.

MERCY CORPS

MasterCard | MasterCard Center for Inclusive Growth

elan
The Electronic Cash Transfer Learning Action Network