ANNEX 1: MODEL PRIVACY IMPACT ASSESSMENT (PIA)

About this Model PIA

A Privacy Impact Assessment looks into an organisation's procedures and technologies to analyse how personal information is collected, used, disseminated, and maintained. It is designed to ensure an organisation incorporates privacy into the development, design and deployment of a technology or policy.

There are a number of methodologies for Privacy Impact Assessments and approaches. This Model PIA is adapted from the PIA developed by the U.S. Department of Homeland Security (DHS). For many years, the DHS has conducted PIAs for all new technologies and rules. In fact, this process is considered to be inherently necessary for all U.S. Federal Government programmes since 2002, as required by the E-Government Act of 2002. According to the DHS,

"The purpose of a PIA is to demonstrate that program managers and system owners have consciously incorporated privacy protections throughout the development life cycle of a system or program. This involves making certain that privacy protections are built into the system from the initiation of development, not after the fact when they can be far more costly or could affect the viability of the project."

Rather than merely being an assessment and report of whether an organisation has adhered to principles, the PIA is in itself part of a process that enables organisations to consider the likely implications of new technologies, techniques, and policies so that it can foresee the risks, determine likely problems, and initiate the process of negotiating solutions before they become too complex.

As a result, a PIA is intended to first determine system risks and then consider risk mitigation strategies that can then be fed back into the technology- and policy-making processes. By using a methodology that includes engaging with stakeholders, a PIA itself becomes a method of anticipating and addressing risk, and communicating the challenges to stakeholders and throughout the organisation, and in turn of enhancing confidence. It is for this reason that the Department of Homeland Security sees a PIA as "a living document that needs to be updated regularly as the program and system are changed and updated, not just when the program or system is deployed."

When to do a PIA

The DHS prescribes a privacy threshold review process for determining when a PIA needs to be conducted, which is premised on an exploration of whether and how the programme involves the collection, generation or retention of personal information. For the purposes of this Model PIA, it is assumed that all humanitarian sector programming involves the processing of personal information in some way and there is thus a prima facie need for a PIA.

MODEL PRIVACY IMPACT ASSESSMENT FOR HUMANITARIAN OPERATIONS

1 Information

What information is collected, used, disseminated, or maintained in the system?

What are the sources of the information?

Why is the information being collected, used, disseminated, or maintained?

How is the information collected?

How will the information be checked for accuracy?

What specific legal authorities, arrangements, and/or agreements defined the collection of information?

Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they have been mitigated.

2 Uses

Describe all uses of the information.

What types of tools are used to analyse the data and what type of data may be produced?

If the system uses commercial or publicly available data please explain why and how it is used.

Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above-described uses.

3 Retention

How long is information retained?

Has the retention period been approved?

Privacy Impact Analysis: Discuss the risks associated with the length of time data is retained and how those risks have been mitigated.

4 Internal Sharing and Disclosure

With which internal organisation(s) is the information shared, what information is shared and for what purpose?

How is the information transmitted or disclosed?

Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they have been mitigated.

5 External Sharing and Disclosure

With which external organisation(s) is the information shared, what information is shared, and for what purpose?

Is the sharing of personally identifiable information outside the organisation compatible with the original collection?

If so, is it covered by an appropriate policy and notice statement?

How is the information shared outside the organisation and what security measures safeguard its transmission?

Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they have been mitigated.

6 Notice

Was notice provided to the individual prior to the collection of information?

Do individuals have the opportunity and/or right to decline to provide information?

Do individuals have the right to consent to particular uses of the information? If so, how does an individual exercise that right?

Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

7 Access, Redress and Correction

What are the procedures that allow individuals to gain access to their own information?

What are the procedures for correcting inaccurate or erroneous information?

How are individuals notified of the procedures for correcting their information?

If no formal redress is provided, what alternatives are available to the individual?

Privacy Impact Analysis: Discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

8 Technical Access and Security

What procedures are in place to determine which users may access the system and are they documented?

Will organisational contractors have access to the system?

Describe what privacy training is provided to users either generally or specifically relevant to the programme or system?

What auditing measures and technical safeguards are in place to prevent misuse of data?

Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

9 Technology

What type of project is the programme or system?

What stage of development is the system in and what project development life cycle was used?

Does the project employ technology which may raise privacy concerns? If so please discuss its implementation.