

Using PIM to Enhance the Understanding of Data Protection Risks in Food Security Programming

Regional Protection Advisor for the World Food Programme, Fausto Arya De Santis, explains how the PIM Initiative and the PIM Framework influenced his way of thinking and improved his advice on responsible information management in his role with WFP.

Fausto Arya De Santis is a Regional Protection Advisor for the World Food Programme (WFP). He participated in a PIM training in 2018 while working as a Protection Advisor for WFP in Afghanistan.

Relevance of the PIM Framework for the World Food Programme (WFP)

According to Fausto, the PIM Conceptual Framework and the PIM training are not just useful for protection agencies and protection programmes. They helped shape his thinking and practice in his role with WFP:

The information, the tools, the way of thinking and the analysis suggested by PIM was very useful not just for protection information, but also generally to understand what data was sensitive, why and how; to understand the risks and understand what mitigating measures can be put in place. It also highlighted the interdepartmental work and ... responsibility in such things, [that it is] not just [the responsibility of one] person or [one] unit at WFP.

[Issues of data protection, privacy and sensitive data in humanitarian response are] becoming increasingly important not only for our own [WFP] operations within large scale emergencies and the intersection between sensitive information and [issues of] access and do-no-harm, but also where we support more development work around social protection schemes and the type of data and beneficiary data management processes governments are interested in... All of these [processes] require data sharing agreements and these agreements need to be based on Privacy Impact Assessments and the understanding of risks associated with the various data fields.

The PIM training... helped me better understand the field [of responsible information management] and provide more informed support when I was asked to.

Data collection at WFP

Fausto describes this further in relation to his work on the roll-out of WFP's beneficiary information and transfer management platform, SCOPE, as well as Privacy Impact Assessments (PIAs):

I remember using the way of thinking and the processes demonstrated by PIM to try and understand within our own operations what risks could exist. At that point in time we were rolling out WFP's beneficiary information and transfer management platform called SCOPE, so [we were] then trying to see which data fields [were needed], what type of data sharing, with who, why, how it would affect access, who could be interested.

... The WFP SCOPE software... captures beneficiary information, [including] biometrics, such as fingerprints and iris scan. It can be used [by WFP and other agencies] to provide assistance, irrespective of modality [cash, voucher, in-kind, WFP card, etc.].

By the time of the PIM training, it was [being introduced in] Afghanistan. The other person who came along to the PIM training was the person in charge of the rollout of SCOPE. ... [and] PIM helped us to better structure our ideas and initial analysis and we started thinking about drafting privacy impact assessments.



SCOPE card reader and biometric scanner in use

A privacy impact assessment looks at the context, the legal frameworks, the data flows and the protection environment to identify what are the risks associated with data, primarily personal identifiable data, in a certain activity in a certain context, in a certain project or partnership. Often it ends up being the responsibility of protection focal point or officer or advisor because protection risks are a key component, but it doesn't have to be. Ultimately, the PIA [identifies] risks and mitigating measures.

Risks Associated with WFP Data Collection

Fausto explained that, in undertaking risk analyses, WFP in Afghanistan did not specifically use the PIM Framework:

...What we saw value in [in the PIM Framework] was more around the analysis... In terms of risks of utilising SCOPE in Taliban-controlled areas, there were issues [around] what government or non state armed actors would be interested in having, so what to collect and what not to collect and how that would affect potential access issues; who has access to [the data] and potential rumours around [data collection processes]...[Across Afghanistan], [capturing] religion or land ownership and these kinds of very sensitive types of information... definitely before capturing any of this we need to understand the risks around ...these data fields.

WFP Initiatives that reflect PIM Principles

Other WFP initiatives reflected PIM Principles, although, again, may not have been a specific outcome of applying the PIM Framework:

[Another] of the things we were working on when I was in Afghanistan was informed consent and [developing] the text that enumerators would have to read to beneficiaries before registering them. This included discussing with programme managers about the procedures that needed to be in place so people who don't consent to biometrics can receive assistance without providing fingerprints.

[We also had] focus group discussions to specifically discuss data risks with some communities.

Influence of PIM on ways of thinking and provision of feedback

The PIM training was very valuable to understand the basic principles of responsible information management that we see more and more in the area of data privacy and protection, also in terms of understanding the context and what are the risks associated with what kind of data.

A lot of the information that I received from the training and the learnings from it were valuable for me to provide more informed feedback to HQ when they were developing tools for WFP on beneficiary data management, including [Privacy Impact Assessments]. It also helped me to conceptually better structure PIAs before we had a proper tool and to be able to better develop the PIA once we did have a tool.

PIM Highlights

- Emphasis on data protection and security, which helped shape privacy impact assessments ([PIM Principle](#) - data responsibility, protection and security)
- Sought to clarify purpose of data collection (PIM principle - Defined Purpose)
- Sought to avoid risks relating to beneficiary information management system (PIM Principle - Do No Harm)
- Developed mechanisms so that lack of consent to data collection was not a barrier to assistance therefore ensuring systems were people-centred (PIM Principles - Informed Consent, People-centred and inclusive)
- Engaged communities in discussions on data risks ([PIM Matrix](#) - Communicating with Communities; PIM Principles – Do no harm and People-centred and inclusive)