Mitigating risks of abuse of power in cash assistance

TOOLS: Protecting cash recipients' personal data

KEY ACTIONS

In cash assistance, the personal data of cash recipients can be exchanged with a vast number of parties (humanitarian organisations, government entities, financial service providers including their agents, traders). At any stage of these exchanges, data breaches may occur. It is therefore paramount to put in place adequate standards:

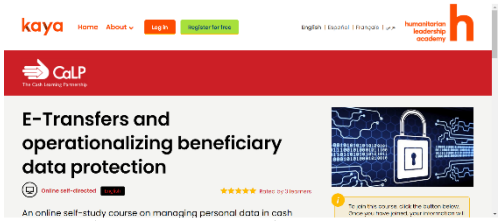
- Ensure that personal information is safeguarded.
- Advocate for the development/application of data protection frameworks that support the lean collection of personal information and efficient processing and redress.
- If necessary, conduct data privacy impact assessments of your programmes.

Practical steps in this regard need not be onerous and can include, for example:

- Keeping data of preceding clients from view of other clients by covering logbooks at agent kiosks with a paper.
- Enforcing with FSPs that agents taking pictures of cash recipient for SIM card registration delete these pictures from their phone before leaving the transit/cash distribution site.

TOOL: CALP online course "E-transfers and operationalizing beneficiary data protection"

What is in this tool?	This 5-module course explores the necessary steps to operationalize the protection of beneficiary data in programmes using electronic transfers, or e-transfers. The course includes case studies and experiences from a number of organisations and sector specialists that highlight the risks, challenges and emerging solutions.
How?	Self-study. Of particular interest is Module 4 on Emerging Solutions: This module introduces a number of good practice approaches that your agency can put in place to overcome some of the challenges related to the protection of beneficiary data in e-transfer programmes.

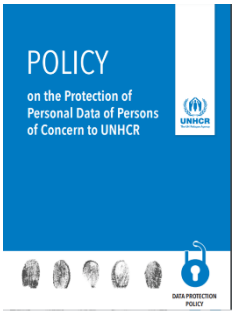


GUIDANCE: UNHCR data protection policy

What is in this tool?	The purpose of this policy is to ensure that UNHCR processes personal data in a way that is consistent with the 1990 United Nations General Assembly's Guidelines for the Regulation of Computerised Personal Data Files and other international instruments concerning the protection of personal data and individuals' privacy.
How?	You should familiarise yourself with this policy which lays down in simple terms the rules and principles related to the processing of personal data of crisis-affected people. You can use it to raise awareness of other stakeholders on the importance of data protection.
When?	During the strategic planning phase or during implementation and monitoring.

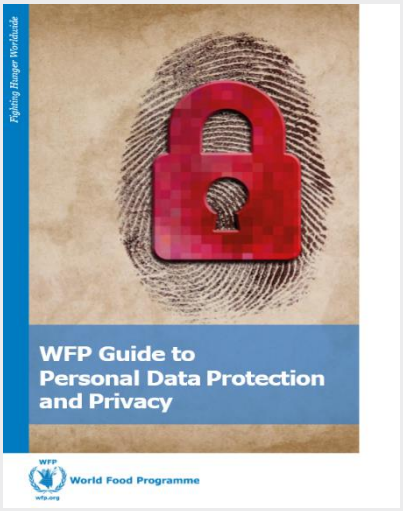
Particularly relevant to mitigating risks of abuse of power is developing an understanding of:

- The rights of data subjects (p. 18)
- Data processing by UNHCR (p. 24)
- Data processing by implementing partners (p. 30)
- The transfer of personal data to third parties (p. 34)
- Accountability and supervision (p. 40)



GUIDANCE: WFP Guide to Personal Data Protection and Privacy

What is in this tool?	This guidance highlights the principles and operational standards for the protection of cash recipient personal data in WFP's programming based on 5 data protection principles: 1. Lawful and Fair Collection and Processing; 2. Specified and Legitimate Purpose; 3. Data Quality; 4. Participation and Accountability; and 5. Security.
How?	You must ensure that you understand and address (through a Privacy Impact Assessment – PIA) the protection risks arising from the processing of beneficiary personal data in the context of the local legislation and regulations related to personal data in your country of operation. This may require that you perform a partner due diligence with a specific focus on their minimum data protection safeguards. It is best practice to adhere to the data minimisation principle. This includes only sharing the necessary data and ensuring partners delete or return data at the end of the programme or once the legitimate purpose has been achieved, unless otherwise consented to by data subjects. This requires that you have in place a data protection contract with the partner.
When?	Before collecting and sharing personal data for programme implementation.



Further reading:

CASE STUDY: ICRC: The Humanitarian Metadata Problem: "Doing No Harm" in the Digital Era

This document addresses the increase in exchange of metadata as mobile telecommunications, messaging apps and social media are used by humanitarians to coordinate responses, communicate with employees and engage affected populations. To reconcile the growing amount of metadata with the "do no harm" principle, the humanitarian community must better understand the risks associated with the generation, exposure and processing of metadata. This study looks at how this is particularly important for organisations, such as the United Nations, that enjoy certain privileges and immunities but are not able to counter these risks alone. This study can also help you map who exactly has access to the data and metadata created during such exchanges and for how long. These factors are affected by the technical, legal and policy landscapes, which vary greatly despite efforts to streamline regulations.