12. DATA PROTECTION PRINCIPLES

1 RESPECT

Principle: Organisations should respect the privacy of beneficiaries and recognise that obtaining and processing their personal data represents a potential threat to that privacy.

2 PROTECT BY DESIGN

Principle: Organisations should "protect by design" the personal data they obtain from beneficiaries either for their own use, or for use by third parties for each cash or e-transfer programme they initiate or implement.

3 UNDERSTAND DATA FLOWS AND RISKS

Principle: Organisations should analyse, document and understand the flow of beneficiary data for each cash or e-transfer programme they initiate or implement within their own organisation and between their organisation and others and develop risk mitigation strategies which might be required to address any risks arising from these flows;

4 QUALITY AND ACCURACY

Principle: Organisations should ensure the accuracy of the personal data they collect, store and use, including by keeping information up to date, relevant and not excessive in relation to the purpose for which they are processed, and by not keeping data for longer than is necessary.

5 OBTAIN CONSENT OR INFORM BENEFICIARIES AS TO THE USE OF THEIR DATA

Principle: At the point of data capture, beneficiaries should be informed as to the nature of the data being collected, who it will be shared with, who is responsible for the secure use of their data and be provided with the opportunity to question the use made of the data and withdraw from the programme should they not wish their personal data to be used for the purposes described.

6 SECURITY

Principle: Organisations should implement appropriate technical and operational security standards for each stage of the collection, use and transfer and use of beneficiary data to prevent unauthorised access, disclosure or loss and in particular any external threats should be identified and actions taken to mitigate any risks arising.

7 DISPOSAL

Principle: Organisations should not hold beneficiary data for longer than is required unless they have clear, justifiable and documented reasons for doing so otherwise data held by the organisation and any relevant third parties should be destroyed.

8 ACCOUNTABILITY

Principle: Organisations should establish a mechanism whereby a beneficiary can request information about what personal data an organisation holds about them, and mechanisms to receive and respond to any complaints or concerns beneficiaries may have about the use of their personal data.

Source: CaLP (2013) *Protecting Beneficiary Privacy: Principles and Operational Standards for the Secure Use of Personal Data in E-Transfer Programmes.*