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.

ANNEX 2: MODEL CLAUSES TO CONTRACTS WITH THIRD PARTIES

A: BENEFICIARY NOTICE AND CONSENT (PLAIN LANGUAGE TEMPLATE)

Agreement on Personal Data

Case/Identifying Number	
Name of Beneficiary	
Date	
Place	

How form will be explained

Name of Person Explaining Form	
Role of Person Explaining Form *(e.g. case officer/volunteer)*	
Explanation by person filling in form will be in *(language of explanation by person filling in form)*	
and translated into *(language that explanation will be made in to beneficiary)*	

Explanation will be assisted by

1. Translation by trained Interpreter *or*

2. Informal Translation by _____

(record name of translator and relationship to beneficiary e.g. sister, priest)

3. Assistance by trusted party _____

(record name of translator and relationship to beneficiary e.g. sister, priest)

If you want to be part of the [insert name of programme] then we need to ask you some questions. We use what you tell us about yourself to organise how you get the [insert benefit in programme/cash payment]. There are rules about what we can do with what you tell us. What you tell us is called personal data. These are the rules.

1. We can only use your personal data to do the things that you agree today. We want to use your data to run the [insert name of programme]. We use your personal data to:
    - get the [name of benefit in programme/cash payment] to you;
    - stop the money being stolen;
    - learn how to make the [insert name of programme] better.
    - [Optional: include other benefits from [insert name of agency]

We can only keep your personal data as long as we need it to do these actions. If we want to do something different with your personal data then we must talk to you again.

2. The personal data that we will ask you to give us today is [insert categories of data e.g. name, mobile phone number, the data itself may be recorded on a separate form but that must be filled in only after this consent is obtained.]

3. We do share your personal data with others so that you can get the [name of benefit in programme/cash payment]. We will share it with [insert name of service provider e.g. bank or mobile network] or other [insert providers details] to get the [name of benefit in program/cash payment] to you. When we share your personal data with these others they must also obey these rules. They are not allowed to use your personal data to sell you things, just to give [name of benefit in programme/cash payment] to you. You can always ask us with whom we have shared your information.
4. We try our best to look after your personal data so that no one else can use it except for those with whom we share it. Everyone who gets your personal data from us must try their best to look after it.
5. There is a risk that someone else could get your personal data from us by doing wrong. [If there is a significant threat that a governmental or other entity might obtain the data with negative consequences beyond breach of data privacy for the beneficiary, then the person filling in the form should explain the threat at this point. It is not recommended that the nature of the threat be recorded since that might trigger retaliation against the organisation collecting the data to facilitate payment.]
6. We might have to give your personal data to a government because of laws.
7. If you think that we or someone that we have shared your personal data with has got it wrong then you can tell us to make it right.
8. If some of your personal data changes you can get us to change it.
9. If you think that we or someone that we have shared your personal data with has broken the rules you can complain to us. [Insert contact details of person in country responsible for ensuring compliance with Code of Conduct].

Recording Agreement

Now that you have heard these rules about what we do with your personal data, do you agree to give us your personal data?

Yes ☐ No ☐

If yes then indicate how the beneficiary agrees.

1. Signing a copy of this form.

Signature _____

2. Making a thumbprint or fingerprint on a copy of this form.

Fingerprint ☐

3. Making a mark next to his or her name. Name and mark: _____

4. Other way (write how the beneficiary agreed): _____

If no then explain to the beneficiary that there is another way to get the benefit and what it is, or if there is no other way then explain to the beneficiary that there is no other way.

B: AID AGENCY AND E-TRANSFER SERVICE PROVIDER

Overview:

The Model clauses provide for the following:

- establishing that the aid agency (the Agency) is the "Data Controller" – the initiator of the request for data processing
- the e-transfer service provider is the "Data Processor"
- the e-transfer beneficiary who discloses their personal data to the Agency is the "Data Subject"
- that the Data Processor can only process the data for the purposes of the contract (which need to be express) and under the written instruction of the Data Controller
- that the Data Processor must not disclose the data to any third party or subcontract to any third party without the consent of the Data Controller, and must have adequate internal information security standards to prevent unauthorised access, processing or disclosure of data
- agreement as to what happens to the data at the end of the contract
- limitations on the Data Processor's use of data for marketing, profiling and other commercial uses not aligned with processing authorised by the Agency
- limitations on contact with the Data Subjects (beneficiaries) i.e. all contact with the beneficiaries shall be through the Agency, unless otherwise agreed between the Agency and the third party
    - that the Data Processor shall ensure that its personnel and sub-contractors acting under the direct or indirect control of the Data Processor in performance of the Data Processor's duties to the Agency contractually agree to:
    - Comply with non-disclosure obligations to ensure the confidentiality of the data
    - Comply with relevant data processor policies such as Privacy Policy, Security Policy aimed at complying with the Data Processor's duties to safeguard the data
    - Comply with obligations to maintain the quality of the data handled by the relevant personnel and sub-contractors including the accuracy of the data

The clauses represent a minimum standard but may be amended by the relevant Agency (i) to accommodate variations in terminology and naming conventions in the data protection laws applicable to the countries; or (ii) to adopt higher standards of data protection; or (iii) to accommodate specificities in the engagement between the particular Agency (Data Controller) and Data Processor.

It is important to note, that over and above the requirements of the 'Principles and Operational Standards for the secure use of personal data In cash and e-transfer programmes', data protection laws in several countries provide that even where a Data Processor causes a loss or unauthorised disclosure of Personal Data, it is the Agency, the Data Controller, who will be ultimately responsible for the breach. Hence the Data Controller may be civilly or criminally liable for data protection breaches occasioned by the Data Processor. The Agency has an interest, therefore, in adopting measures additional to the agreement to procure the Data Processor's technological and organisational compliance with the agreement such as auditing the Data Processor's compliance with the agreement or periodic reporting by the Data Processor on the privacy and security policies and procedures implemented by the Data Processor.

MODEL CLAUSES

The Model Clauses below are drafted so as to constitute a distinct agreement and **will require negotiation and editing**. The clauses may however be inserted into master/main agreements which govern other aspects of the relationship between Agency and Affiliate/Service Provider.

AGREEMENT BETWEEN:

1 [Name of Agency], having its registered office at […] (the "Data Controller"); and

2 [Name of Affiliate/ Service Provider], having its registered office at […] (the "Data Processor").

PURPOSE OF THIS AGREEMENT

A For the purpose of facilitating electronic cash transfers from the Data Controller to a beneficiary receiving the cash transfer, the Data Controller collects and processes the Personal Data of such beneficiaries.

B The Data Controller has engaged the Data Processor to render the Services which includes processing beneficiary data on the Data Controllers' behalf.

C The Data Controller is subject to laws, regulations and codes of conduct, principles and operational standards that place obligations on the Data Controller to respect the privacy and protect the Personal Data of beneficiaries in the processing of such data, whether independently or through appointed Data Processors.

D Accordingly, this agreement pertains to the protection of Personal Data accessed or otherwise received; and processed by the Data Processor on the Data Controller's behalf in the course of rendering the Services.

IT IS AGREED:

1 DEFINITIONS AND INTERPRETATION

1.1 In this agreement:

Data Controller means the Agency being the person who determines the purposes for which and the manner in which any Personal Data is, or is to be, processed.

Data Processor means the Affiliate/ Service Provider, a person who processes Personal Data on behalf of the Data Controller during the course of rendering the Services.

Data Subject means the beneficiaries of electronic cash transfers facilitated by the Agency and persons to whom the Personal Data refers.

Personal Data means any personal information including identifying information such as the name, identification or passport number, mobile telephone number, email address, cash transaction details, of whatever nature, format or media that by whatever means, is provided to the Data Processor by the Data Controller, is accessed by the Data Processor on the authority of the Data Controller or is otherwise received by the Data Processor on the Data Controller's behalf and includes transactional or other information associated with the Data Subject generated by the Data Processor in the course of providing the Service to the Data Controller.

Processing in relation to Personal Data, includes the obtaining, recording or holding of such data or carrying out any operation or set of operations on the data, including organisation, adaptation, or alteration; disclosure by transmission, dissemination, or otherwise; and alignment, combination, blocking, erasure, or destruction.

Schedule means the schedules annexed to and forming part of this agreement.

Services means the specific activities for which the Data Controller has engaged the Data Processor as set out in Schedule A [or clause […] of main/ master agreement]

2 DATA PROCESSING

2.1 The Data Processor agrees to process the Personal Data to which this agreement applies, and in particular the Data Processor agrees that it shall:

a. process the Personal Data in accordance with the terms and conditions set out in this agreement and where the standards imposed by the data protection legislation regulating the Data Processor processing of the Personal Data are higher than those prescribed in this agreement, then in accordance with such legislation;

b. process the Personal Data strictly in accordance with the purposes relevant to the Services in the manner specified from time to time by the Data Controller; and for no other purpose or in any other manner except with the express prior written consent of the Data Controller;

c. implement appropriate technical and organisational measures to safeguard the Personal Data from unauthorised or unlawful processing or accidental loss, destruction or damage, having regard to the state of technological development and the cost of implementing any measures; such measures shall ensure a level of security appropriate to the harm that might result from unauthorised or unlawful processing or accidental loss, destruction or damage and to the nature of the Personal Data to be protected;

d. regard the Personal Data as confidential data and not disclose such data to any person other than to employees, agents or sub-contractors to whom disclosure is necessary for the performance of the Service and subject to […] below or except as may be required by any law or regulation affecting the Data Processor;

e. implement technical and organisational measures to ensure the confidentiality, privacy, integrity, availability, accuracy and security of the Personal Data including establishing organisational policies for employees, agents and sub-contractors aimed at complying with the Data Processor's duties to safeguard the Personal Data in accordance with this agreement;

f. implement backup processes as agreed between the Data Controller and Data Processor to procure the availability of the Personal Data at all times and ensure that the Data Controller will have access to such backup of the Personal Data as is reasonably required by the Data Controller;

g. ensure that any disclosure to an employee, agent or sub-contractor is subject to a binding legal obligation to comply with the obligations of the Data Processor under this agreement including compliance with relevant technical and organisational measures for the confidentiality, privacy, integrity, availability, accuracy and security of the Personal Data. For the avoidance of doubt, any agreement with an employee, agent or sub-contractor shall not relieve the Data Processor of its obligation to comply fully with this agreement, and the Data Processor shall remain fully responsible and liable for ensuring full compliance with this agreement;

h. comply with any request from the Data Controller to amend, transfer or delete Personal Data; provide a copy of all or specified Personal Data held by it in a format and or a media reasonably specified by the Data Controller within reasonable timeframes as agreed between the parties [Agency to insert relevant time periods at its discretion];

i. should the Data Processor receive any complaint, notice or communication which relates directly or indirectly to the processing of the Personal Data or to either party's compliance with applicable law, immediately notify the Data Controller and provide the Data Controller with full co-operation and assistance in relation to any complaints, notices or communications;

j. promptly inform the Data Controller if any Personal Data is lost or destroyed or becomes damaged, corrupted or unusable and at the request of the Data Controller, restore such Personal Data at its own expense;

k. in the event of the exercise by Data Subjects of any rights in relation to their Personal Data, inform the Data Controller as soon as possible,

l. assist the Data Controller with all Data Subject information requests which may be received from any Data Subject in relation to any Personal Data;

m. not use the Personal Data of Data Subjects to contact, communicate or otherwise engage with the Data Subjects including transmission of any marketing or other commercial communications to the Data Subjects, except in accordance with the written consent of the Data Controller or to comply with a court order. For the avoidance of doubt, the Data Processor is not prohibited from contact, communication or engaging with the Data Subject in so far as this does not involve processing of Personal Data and the Data Processor ensures that the promotion or offer of services is not in any manner associated to the Data Controller or the Data Controller's services;

n. notify the Data Controller of the country(s) in which the Personal Data will be processed where such country(s) is not the country of the Data Processor's registered office;

o. not process or transfer the Personal Data outside of the country of its registered office except with the express prior written consent of the Data Controller pursuant to a request in writing from the Data Processor to the Data Controller;

p. permit and procure that its data processing facilities, procedures and documentation be submitted for scrutiny by the Data Controller or its authorised representatives, on request, in order to audit or otherwise ascertain compliance with the terms of this agreement;

q. advise the Data Controller of any significant change in the risk of unauthorised or unlawful processing or accidental loss, destruction or damage of Personal Data; and

r. report [in accordance with agreed reasonable timeframes] to the Data Controller on the steps it has taken to ensure compliance with clause 3.1.of this agreement.

3 WARRANTIES

3.1 The Data Processor warrants that:

a. it will process the Personal Data in compliance with laws, enactments, regulations, orders, standards and other similar instruments applicable to the Data Processor; and in accordance with the terms and conditions of this agreement;

b. in order to observe the rights of ownership and/or other proprietary or intellectual property rights of the Data Controller in the Personal Data, not copy, retain or process the Personal Data in any manner over the course of this agreement and upon expiration or termination of this agreement, except as required by law or in accordance this agreement.

4 INDEMNITY

4.1 The Data Processor agrees to indemnify and keep indemnified and defend at its expense the Data Controller against all costs, claims, damages or expenses incurred by the Data Controller or for which the Data Controller may become liable due to any failure by the Data Processor or its employees, subcontractors or agents to comply with the obligations under this agreement.

5 APPOINTMENT OF SUB-CONTRACTORS AND AGENTS/ COMPLIANCE BY SUB-CONTRACTORS AND AGENTS

5.1 The Data Processor may authorise a third party (sub-contractor or agent) to process the Data:

a. subject to the terms of this agreement;

b. subject to the Data Controller's prior written consent, the validity of the consent will be conditional on the Data Processor supplying the Data Controller with full and accurate details of the sub-contractors or agents; and

c. provided the relevant sub-contractor's or agent's contract terminates automatically on the termination of this agreement for any reason.

6 TERMINATION

6.1 This agreement shall terminate automatically upon termination or expiry of the Data Processor's obligations in relation to the Services.

6.2 The Data Controller shall be entitled to terminate this Agreement forthwith by notice in writing to the Data Processor if:

a. the Data Processor is in a material or persistent breach of this Agreement which, in the case of a breach capable of remedy, shall not have been remedied within […] days from the date of receipt by the Data Processor of a notice from the Data Controller identifying the breach and requiring its remedy; or

b. the Data Processor becomes insolvent, has a receiver, administrator, or administrative receiver appointed over the whole or any part of its assets, enters into any compound with creditors, or has an order made or resolution passed for it to be wound up (otherwise than in furtherance of a scheme for solvent amalgamation or reconstruction).

6.3 On termination of this agreement the Data Processor shall, in accordance with the direction of the Data Controller:

- deliver or destroy all Personal Data supplied by the Data Controller in its possession or under its control;
- instruct all its employees, agents and sub-contractors to facilitate and ensure the delivery or destruction of the Personal Data including copies of the Personal Data in accordance with the Data Controller's direction.

7 GOVERNING LAW

7.1 This agreement will be governed by the laws of […], and the parties submit to the exclusive jurisdiction of the Courts of […] for all purposes connected with this agreement, including the enforcement of any order or judgment made under or in connection with it.

8 WAIVER

8.1 Failure by either party to exercise or enforce any rights available to that party or the giving of any forbearance, delay or indulgence shall not be construed as a waiver of that party's rights under this agreement.

9 INVALIDITY

9.1 If any term or provision of this agreement shall be held to be illegal or unenforceable in whole or in part under any enactment or rule of law, such term or provision or part shall to that extent be deemed not to form part of this agreement, but the enforceability of the remainder of this agreement shall not be affected, provided however that if any term or provision or part of this agreement is severed as illegal or unenforceable, the parties shall seek to agree to modify this agreement to the extent necessary to render it lawful and enforceable, and as nearly as possible to reflect the intentions of the parties embodied in this agreement, including without limitation the illegal or unenforceable term or provision or part.

CaLP
The Cash Learning Partnership

These principles and operational standards have been produced by CaLP in collaboration with a large number of agencies and key stakeholders to enable agencies to address risks inherent in the use of beneficiary data by agencies engaged in delivery of cash with a specific focus on e-transfer programmes.

These risks are associated with the collection, storage, use and disclosure of beneficiary data in receipt of cash and e-transfers. This personal data is often more extensive than that gathered in conventional aid distributions and is necessarily shared with, or generated by, commercial partners who assist in the distribution of cash via new technological means.

These risks have, on the whole, gone unrecognized and unaddressed by humanitarian actors. However, as humanitarian initiatives increasingly adopt new technologies to improve the effectiveness of aid delivery, it is vital that standards are put in place to ensure that beneficiaries are put at risk or disadvantaged by their involvement in cash transfer programmes.

These principles and operational standards are an attempt to establish good practice within the sector for the collection and processing of beneficiary data. They are specifically addressed to managers of cash and e-transfer programmes but can have a wider application. They are not intended to replace or be a substitute for existing organizational data protection or privacy policies but can enhance or compliment such policies where these policies do not include protections for beneficiary data or they lack detail. Where organizational privacy or data protection policies do not exist they offer a framework for protecting beneficiary data.

The principles and operational standards include eight *Principles* governing how data should be processed and steps that agencies can take to adhere to them in the form of *Operational Standard interpretative Notes*. Model clauses for beneficiary are provided for agency adaptation.

This research was commissioned by the Cash Learning Partnership (CaLP),
with the generous support of VISA Inc. and DFID

VISA

UKaid
from the British people