PROTECTING BENEFICIARY PRIVACY

Principles and operational standards for the secure use of personal data in cash and e-transfer programmes

CaLP
The Cash Learning Partnership

BACKGROUND TO THE PRINCIPLES

The use of electronic transfers (e-transfers) in cash transfer programming (CTP) has grown in the humanitarian sector and is increasingly recognised as an effective and efficient intervention in certain emergency contexts. Following recommendations made in Cash Learning Partnership (CaLP) research in 2011 on e-transfers 'New Technologies in Cash Transfer Programming and Humanitarian Assistance'[1] (Smith G et al 2011) and demonstrated interest from the CaLP community of practice; CaLP has undertaken an additional three pieces of work in this thematic area in 2013, of which this is one. The other two pieces include the development of e-transfer guidelines and a study of factors affecting the cost-effectiveness of e-transfers compared to more manual methods.

E-transfers carry inherent privacy-related risks associated with the collection and handling of beneficiaries' personal data. Yet these risks have largely gone unrecognised and unaddressed. Agency practice is rarely codified, often left to programme teams to manage under the humanitarian watchword of "do no harm", although with limited practical guidance. Recent publications such as 'Humanitarianism in a Network Age' (OCHA 2013) and the ICRC 'Professional Standards for Protection work' (2013) highlight this concern.

Informed by this context, CaLP embarked on the development of a set of principles and operational standards that aim to support ethical cash and e-transfers, and help ensure principled use of beneficiary data.

The development of the Principles and Operational Standards was led by Koko Sossouvi (independent consultant) with inputs from a wide number of stakeholders including a technical working group. The process included a literature review; including of key humanitarian and industry standards, codes and operational guidelines, as well as instruments related to anti-money laundering and countering the financing of terrorism; an online survey on practitioners' current data management policies and practices; stakeholder mapping; a drafting process; which benefited from legal advice from Oxfam GB, Save the Children UK, ACF/ France. Following the inclusion of comments and recommendations from numerous stakeholders, a round table meeting was held to discuss and debate the content of the penultimate draft document and next steps for their completion and uptake. This document is based on the outcomes of the round table.

Photo: Geoff Sayer/Oxfam

[1] See CaLP website: http://www.cashlearning.org/resources/library/272-new-technologies-in-cash-transfer-programming-and-humanitarian-assistance?keywords=new+technologies&country=all&sector=all&modality=all&language=all&payment_method=all&document_type=all&searched=1&x=0&y=0

Acknowledgements

CaLP would like to acknowledge the contributions and recommendations made by Kokoevi Sossouvi (independent consultant), Mike Parkinson (Oxfam GB), Carly Nyst (Privacy International), Alexander Beck (UNHCR) and Kate Lauer (independent consultant) amongst others in the development of this document.

As a very consultative process was applied to the development of this document, CaLP benefited significantly from the legal and technical experience of a number of people and their organisations including those employed by: IRC, ACF, C-Gap, SMART campaign, Vodafone, GSMA, OpenRevolution, IFRC, NRC and WFP. CaLP would like to thank these people (you know who you are) as well as the wider community of practice for responding to questions related to this work raised on D-Groups.

Members of the Technical Working Group who provided overall oversight, time, energy and support include:

Ruth Aggiss and Jessica Saulle, Save the Children UK

Jenny Aker, Tufts University

Simon Clements, World Food Programme

Olivia Collins, United Nations Children's Fund (formerly with Somalia Cash Consortium)

Hanna Mattinen, United Nations High Commissioner for Refugees

Hamilton McNutt, NetHope

Julien Morel, Action Contre la Faim

Sasha Muench, Mercy Corps

Gabrielle Smith, Concern Worldwide

In addition to the above, the development of this document would not have been possible without the financial assistance from Visa Inc. and DfID.

Next steps

The CaLP is keen to receive feedback from the use of the Principles. Organisations are kindly invited to send their thoughts and share their programme experiences at info@cashlearning.org and join the CaLP discussion group (by using the link on website www.cashlearning.org).

In addition, readers are reminded that there are substantial resources available on the CaLP website; ranging from case studies and reports on the use of new technologies to cash transfer programme (CTP) guidelines, research on the use of CTP, and market analysis.

PROTECTING BENEFICIARY PRIVACY: PRINCIPLES AND OPERATIONAL STANDARDS FOR THE SECURE USE OF PERSONAL DATA IN CASH AND E-TRANSFER PROGRAMMES

A PURPOSE

The right to privacy through the protection of personal data is not only an important right in itself, but also a key element of individual autonomy and dignity. Protecting and respecting privacy is a strong enabler of political, spiritual, religious and even sexual freedoms. A number of international instruments enshrine data protection principles, such as Article 8 of the European Convention on Human Rights and Fundamental Freedoms[2], and many domestic legislatures have incorporated such principles into national law.

These Principles and Operational Standards have been produced by the Cash Learning Partnership (CaLP) to enable agencies to meet and respect these international standards and in particular to address risks inherent in the use of beneficiary data by agencies engaged in the delivery of cash with a specific focus on e-transfer programmes.

These risks are associated with the collection, storage, use and disclosure of the data of beneficiaries 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 unrecognised 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 (who are the very people agencies seek to support) are not exploited, 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. For the reasons stated above, they are specifically addressed to managers of cash and e-transfer programmes but may 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 complement 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.

In view of the wide range of potential jurisdictions in which these Principles and Operational Standards might be applied they can only be advisory and do not constitute legal advice. If in doubt about legal standards which might be applicable then it is recommended that independent legal advice is sought. CaLP has endeavoured to ensure that they meet the requirements of some major legal frameworks but cannot guarantee that some countries' requirements with regard to disclosure, encryption or transfer of data can be met through one set of advisory principles.

[2] See the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108), 1981; the Organization for Economic Co- operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980); and the Guidelines for the regulation of computerized personal data files (General Assembly resolution 45/95 and E/CN.4/1990/72)

B TURNING PRINCIPLES INTO PRACTICE

One of the major challenges in creating this document has been how to produce useful and applicable guidance that practitioners will find useful and relevant to their ways of working while at the same time writing about a regulated activity.

The practitioners consulted in the development of this document wanted guidance which was practical, which addressed the day-to-day reality of programme work often undertaken at times of crisis and operational insecurity and often with beneficiaries in dire need of assistance. Throughout the document, and particularly in relation to the Principles, a balance had to be struck regarding the use of legal frameworks and organisational regulatory language (a request made by compliance officers) and keeping the document practical and approachable to a wider group (practitioner requests). CaLP has attempted to express the key principles in a manner which relates to the way practitioners think in order to make them accessible while at the same time being mindful that processing personal data in many parts of the world is a regulated activity. It is hoped that references in Operational Standards and in the boxes will inform practitioners of the details of the legal framework and satisfy the needs of compliance officers. Feedback[3] from practitioners and compliance officers alike is welcome as we recognise this is a judgement call and one which needs constant oversight.

In addition to relating programme needs to regulatory frameworks we are also conscious that in some circumstances additional costs may be incurred or new skills required to meet the standards set out in this document. Meeting standards is not always cost neutral, although we expect that a great deal can be achieved simply through improved organisation, planning and programme design. For example, some respondents to our consultation process reflected that they "over collect" beneficiary data, others wanted to ensure that when we refer here to operational standards concerning security, these should be integrated into existing institutional resources, such as organisational IT security systems, rather than encourage cash programme teams to design their own security systems.

C DEFINITIONS

For the purposes of this document, personal data is broadly defined *as any data that directly or indirectly identifies or can be used to identify a living individual*. This definition is derived from regulatory frameworks, legislation on client protection and can include personal financial data. By establishing that one of the principles is ensuring the quality and accuracy of data, these principles can be applied to other forms of data such as financial and transactional information, including balances, patterns and timing of expenditure, receipts, rate of activity and so on, which may not always constitute personal data but do relate to operational effectiveness.

D DATA FLOW AND INTER ORGANISATIONAL TRANSFERS

Alongside the secure collection and use of personal data within organisations, the issue of data protection is particularly relevant given the complexity of the flow of data between organisations, whether partner organisations who collect data on behalf of implementing agencies or commercial organisations involved in helping to deliver programmes (see Diagram 1). The elaboration and analysis of data flows alongside the use of Privacy Impact Assessments (see Box 2 and Annex 1) will assist in the risk assessment of the cash transfer programme and we strongly recommend their use.

[3] Email CaLP at info@cashlearning.org, subject area: Principles and Operational Standards

E STATUS OF DOCUMENT AND RECOMMENDATIONS AS TO USE AND APPLICATION

These Principles and Operational Standards have been developed by the Cash Learning Partnership (CaLP) with the financial support of DFID and Visa Inc. Please note that the contents are the responsibility of CaLP and do not necessarily reflect the views of DFID or Visa Inc.

It is intended that they are adopted by non-governmental and inter-governmental agencies which implement cash and e-transfer programmes. However, they can be used in almost any humanitarian programme.

The Principles and Operational Standards are not subject to external monitoring or compliance by CaLP. It is recommended that organisations which adopt these standards use them for internal and/or external audits, evaluations and programme reviews, and publicise their application in public documents such as Annual Reports or on web sites as evidence as to how they have been utilised and attempts have been made to comply with the Principles.

It is recommended that before an organisation adopts these Principles and Operational Standards their Board of Directors, Management Board or Board of Trustees formally resolve to adopt the Principles and establish a mechanism for reviewing and reporting on compliance. It is further recommended to assign organisational focal points for issues relating to data management at a country, regional and headquarters level. A model resolution to achieve this is provided below.

Model resolution for use by Boards of organisations wishing to adopt the Principles:

"It is resolved that [name of organisation] will

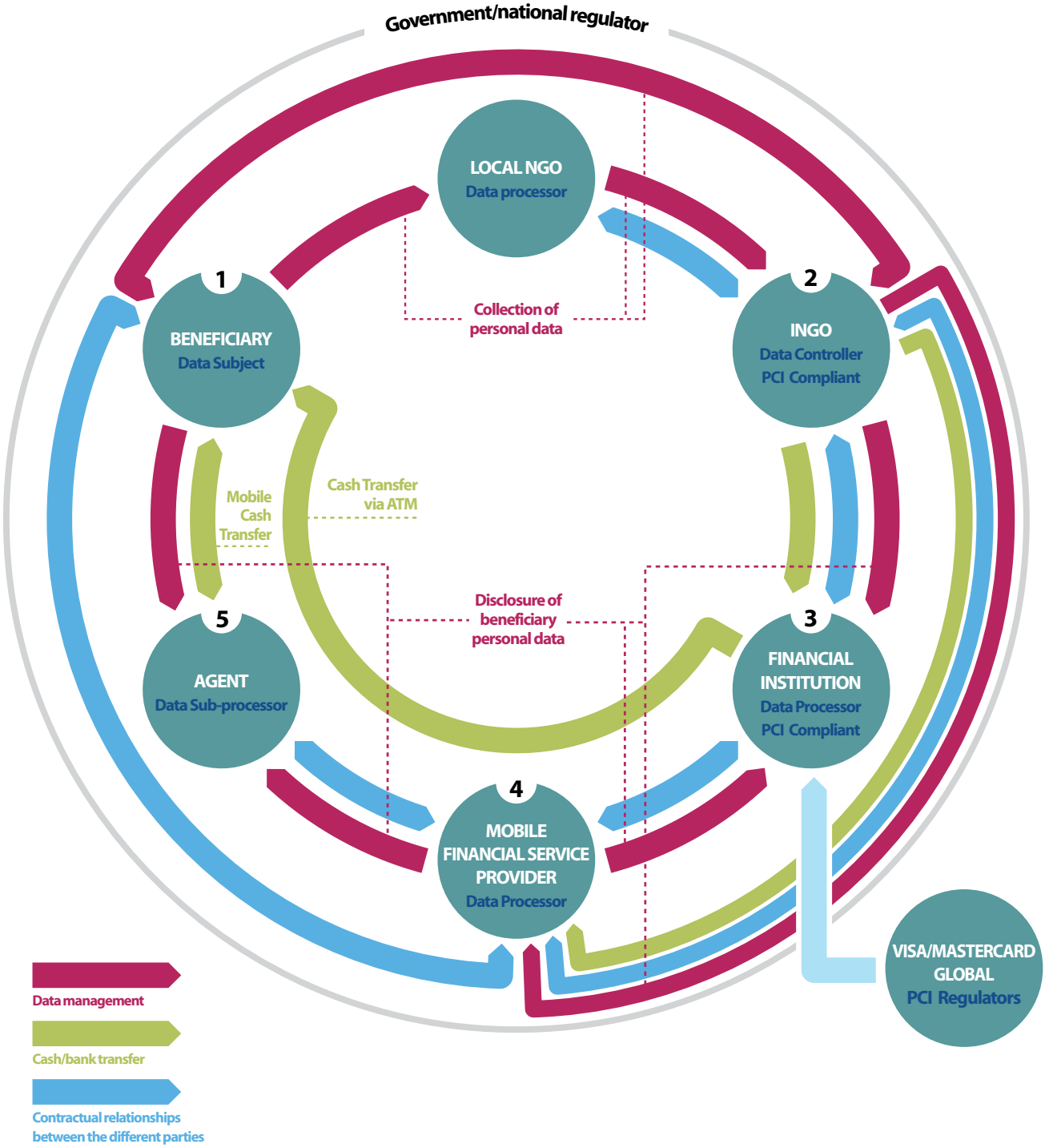
- adopt and implement the Cash Learning Partnership's Principles and Operational Standards for the Secure Use of Beneficiary Data in Cash and e-transfer programmes;
- appoints [name of team or department responsible for implementing the Principles] to ensure that [name of organisation] establishes robust internal procedures to ensure that [name of organisation] complies with the Principles;
- that adoption of and compliance with the Principles is included in [name of organisation's] annual report;
- that the [Board of Management etc] is informed of any serious breaches of the Principles
- that adoption of and compliance with the Principles is subject to periodic review by the [Board of Management etc].

G MAINTAINING STANDARDS AND FEEDBACK

Organisations adopting these Principles are requested to inform CaLP that they have done so. This will enable CaLP to maintain a database of organisations which have adopted the Principles as it is intended to keep this document under review. It would also be helpful to CaLP if organisations which adopt these Principles and Operational Standards could report back on their experience of adopting the Principles and implementing the Operational Standards. This can be done at info@cashlearning.org (please use subject area: Principles and Operational Standards).

As practice evolves and experience is gained the Principles may be amended or strengthened to become an independent Code of Practice or incorporated into other existing standards. CaLP would appreciate any comments on the future application or use of this document.

Diagram 1: Approximation of data flows showing combined view of card-based (ATM) and mobile transfers that are implemented with a local partner



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

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

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

Data sub-processor: the entity to which the data processor delegates all or part of the data processing requested by the data controller.

PCI: Payment Card Industry

PRINCIPLES FOR THE SECURE USE OF PERSONAL DATA IN CASH AND E-TRANSFER PROGRAMMES

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 it is 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, with whom it will be shared, 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 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

OPERATIONAL STANDARDS FOR THE SECURE USE OF PERSONAL DATA IN CASH AND E-TRANSFER PROGRAMMES

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

Operational Standard – interpretive note:

Organisations should:

- Ensure that responsibility for protecting beneficiary data and meeting the standards set out in this document is allocated to a specific post or role within the programme
- Ensure that sufficient resources are allocated to enable this post to function effectively
- Include the steps taken to protect beneficiary data in any monitoring and evaluation of the programme
- Establish mechanisms to inform prospective beneficiaries of who is collecting their data and who is responsible for protecting their data (see Principle 5)
- Only collect personal data by fair and lawful means, if necessary taking legal advice in country as to what national standards might apply

BOX 1: "FAIRLY AND LAWFULLY"

A prerequisite of some Data Protection regulations is the concept that a third party (the "data controller" e.g. the person collecting someone else's data) does so with the consent of the person whose data is being collected (the "data subject") and is done so "fairly and lawfully". The "fairly and lawfully" test is often met when the data subject and data controller enter into a contract for the supply of goods or services which the data subject has requested or the processing is necessary in order to protect the vital interests of the data subject. The application of this concept to aid programmes has not been tested but arguably the provision of aid is both in the vital interests of the data subject and is a commitment by the agency to provide financial support to the beneficiary, even if this is not in the form of a binding contract. Provided that the beneficiaries are informed of the programme and the assistance they may receive and the standards set out under Principle 5 are adhered to, then, in the absence of formal guidance from regulators, it is likely that where regulations require personal data to be "fairly and lawfully" collected, this condition will have been met.

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

Operational Standard – interpretive note:

Organisations should:

- Ensure that issues relating to privacy and the protection of beneficiary data is designed into cash and e-transfer programmes from the beginning, rather than as an "add on" later in the process, to ensure that any potential risks can be addressed in the design process
- Identify in the programme design who is responsible for ensuring compliance with privacy and data protection rules generated by the programme and for reporting and responding to any breaches of the relevant rules
- Agree use of beneficiary data with third parties prior to the programme starting and ensure contractual and controls over the agreed use are included in contracts with third parties
- Where programmatically possible make provisions for beneficiaries who do not want to provide the personal data required to participate in e-transfer programmes, so that they are not excluded from the programme
- Ensure that all staff members receive training on data processing
- Make all reasonable efforts to validate the accuracy of the data with the beneficiary, where organisations receive beneficiary information from sources other than the beneficiary themselves.
- Not allow third parties to use the personal data for purposes other than those needed to deliver the programme or to which the beneficiary has given prior consent
- Not disclose any more beneficiary data than is strictly required by the third party. E.g. Some closed-loop systems under an NGO-held master account can be set up using anonymous sub-accounts whereby the service providers need not receive the name of the sub-account users (as with a gift card)
- Consider the political, legal and social contexts in which the programme is being implemented e.g. be aware of potential local Anti-Money Laundering or Counter-Terrorist Financing regulations or practices that might require the collection of additional personal data, in particular if beneficiary data is likely to be used to vet beneficiaries against terrorist lists or be disclosed to the governments or other organisations (such as financial institutions) or authorities for them to vet against designated lists – see Principle 6 Security

BOX 2: PRIVACY IMPACT ASSESSMENTS

Organisations should consider the benefits of undertaking a Privacy Impact Assessment (PIA) prior to commencing a cash or e-transfer programme. This will help the organisation:

- Identify the privacy risks to individuals
- Identify the privacy and data protection compliance liabilities for the organisation
- Protect the organisation's reputation and instil public confidence in the programme
- Ensure that the organisation is promoting human rights in its humanitarian activities

A model template for a PIA is available in Annex 1.

3 UNDERSTAND DATA FLOWS AND RISK

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

Operational Standard – interpretive note:

Organisations should:

- Analyse the data flows within and between organisations created by the programme and acknowledge where these create risks to beneficiaries' privacy
- Ensure transfers between organisations are secure and subject to written agreement or contract
- Know their partners/third parties' information needs e.g. assess the data needs of any third party involved in the delivery of the programme and their expectations with regard to the ownership and use of data during and at the end of the programme
- Understand when they may be working under contract for a third party to collect information on the third party's behalf e.g. where an agency might be collecting data for a mobile operating network
- Ensure that where organisations operate together in consortia it is agreed and documented within the consortia which organisation is responsible for taking a lead on the protection of beneficiary data and for ensuring adequate protections are built into the design of the consortia's programme so that each agency operates to common standards for ensuring the integrity, protection and use of beneficiary data

BOX 3: MODEL CLAUSES

Throughout this document we refer to arrangements with third parties being subject to contract or to a written agreement. In Annex 2 we have provided model clauses which can be used in contracts with third parties. These are model clauses only and can be used in a variety of ways. As a checklist of issues which a supplier's contract ought to contain, as the basis for negotiation with suppliers or as they stand. It should be recognised that some suppliers may not be able to meet all the conditions in the model clauses as their internal practice and systems may not enable them to agree to all aspects of the clauses.

Photo: Andy Hall/Oxfam

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 it is processed, and by not keeping data for longer than is necessary

Operational Standard – interpretive note:

Organisations should:

- Establish processes for checking the accuracy of all data and mechanisms for keeping data up to date, and for deleting data that is no longer necessary: e.g.:
  - There must be in place a process for ensuring that the data of beneficiaries who have left the programme is deleted both by the organisation and any third parties that have had access to the data, unless the third party has consent to hold that data
- Ensure that the data of beneficiaries who have left the programme is deleted both by the organisation and by any third parties that have had access to that data
- Identify what, if any, information they need to keep at the end of a programme and keep only that data for which there is a legitimate purpose and in the minimum format necessary e.g. legitimate purposes might include possible future programmes, monitoring and evaluation, whereas for research purposes anonymised or aggregated data might be appropriate
- Validate any existing data sets for accuracy and consents before commencing any future programmes
- Ensure that all relevant staff members receive training on data processing.
- Validate the accuracy of data received from sources other than the beneficiaries themselves

Photo: Anna Ridout/ Oxfam

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, with whom it will be shared, 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

Operational Standard – interpretative note

Organisations should:

- Be transparent about how they intend to use the data, and give beneficiaries appropriate privacy notices when collecting their personal data
- Aspire to obtain the active and informed consent of beneficiaries as to the use of their personal data in cash and e-transfer programmes
- Only use alternatives to active and informed consent where obtaining this is impractical. For example legitimate reasons for not seeking active and informed consent might be:
  - Issues of literacy may make obtaining individual consents difficult
  - Urgency – the timetable may not allow for individual interviews to include collection of consents
  - The context of the distribution may make "active and informed consent" meaningless if individuals or families' lives or security are at risk
- Ensure the data is used only for the purpose(s) for which it was collected. Should the purpose(s) change, inform the beneficiary again to seek content

BOX 4: INFORMED CONSENT

As noted under Principle 1 and elaborated in Box 1, some jurisdictions require that personal data must be "fairly and lawfully" processed. The consent of the data subject (i.e.: beneficiary) is one form of making data collection "fair and lawful". Others include where a contract exists or where the data controller has a "legitimate interest". This latter can only be used provided the interests of the data subject are not prejudiced by the processing of their data – hence concerns raised under Principle 6 about the security of personal data.

Practitioners have raised concerns as to the practicality of obtaining the informed consent of beneficiaries in cash or e-transfer programmes. If this is not possible then we consider that beneficiaries should at least be informed individually or collectively or both as to the nature of the programme being provided, what information is being collected, by whom and why. Options include:

- Verbal briefings for individuals/ groups of beneficiaries with the opportunity to ask questions
- As well as a group introduction, using a short statement to be read to the beneficiaries at the point of interview/data capture
- The provision of leaflets or other communications which provide the beneficiary with information about the programme and their rights
- Information about which third parties might access their data and how they can prevent any future unwanted communications from the third party

Always consider the capacity of the beneficiaries to understand and offer consent, and in the case of children or vulnerable individuals or communities, adapt your methodologies appropriately.

A model basic consent form is in Annex 2.

6 SECURITY

Principle: Organisations should implement appropriate technical and operational security standards for each stage of the collection, use and transfer 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

Operational Standard – interpretive note:

Organisations should:

- Ensure that organisational and programme systems are in place to ensure beneficiary data is securely stored, e.g. where possible programme staff should liaise with in-house IT staff on information security
- Be clear who in their programme management team is responsible for data security and put processes in place for the protection of beneficiary personal data from loss, theft, damage or destruction, including back-up systems and effective means to respond to security breaches
- Put processes in place to control who has access to beneficiary personal data and ensure only authorised users can access the data
- Ensure that digital storage systems are encrypted and password protected, and if hard copies of records are retained that include beneficiary data, make sure these records are kept in a secure place
- Ensure that transfers of personal data within and between organisations is only undertaken when required as a programme imperative, is done through secure means and that persons to whom the data is transferred will in turn recognise the confidential nature of the data they receive e.g.
  - Check the track record of private sector partners when it comes to protecting data privacy
- Assess the risks associated with the nature and type of data collected e.g. collection of data of vulnerable groups or communities
- Be aware of local factors that might increase the security risks in relation to e-transfers; such factors might include:
  - Extensive government control of mobile communications, widespread surveillance of phone and internet connections
  - The security vulnerabilities of mobile technologies used to collect, store or transfer data
  - The political, religious, ethnic or social contexts in the country which might create particular risks when collecting and using personal data

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

Operational Standard – interpretive note:

Organisations should:

- Include in their programme exit strategy what personal data they wish to retain and why
- Identify any legal or contractual reasons as to whether or not they need to retain beneficiary data
- Where data is not required, ensure the secure disposal or destruction and/or archive of personal data by all parties that have accessed it, e.g.
  - Take advice from in-house IT staff as to how to securely destroy data
  - Build into data processing systems the capacity to securely destroy data
  - Include specific data deletion procedures in service contracts with the parties with which they intend to share beneficiary data.
  - When supplying beneficiaries with programme hardware such as SIM cards, include automatic opt-out options in contract, should beneficiaries not be willing to maintain a commercial relationship with the service provider at the end of the humanitarian programme.
- Ensure that where the data is required to be held beyond the time-frame previously notified to the beneficiary, or the data is being kept for a purpose different from that originally communicated to the beneficiary, then the beneficiary is informed and, if required, consent from the beneficiaries obtained, i.e. if the purpose has changed significantly then consent as to future use should be obtained

Photo: Simon Rawles

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

Operational Standard – interpretive note:

Organisations should:

- Be aware of any regulatory obligations which apply in the host country with regard to accountability to beneficiaries and beneficiaries rights of access to their personal data
- Establish a mechanism whereby a beneficiary can request information about what information an organisation holds about them, which third parties that information has been shared with and for what purposes it is being used
- Recognise that such systems may carry some costs and allow for such systems in programme budgets
- In line with Principle 2 identify who is responsible for managing and responding to any reported breaches and for onward reporting to their head office and if necessary external regulators
- Brief staff and partners on the requirement to report breaches and any loss of data for which the agency is responsible
- Allow beneficiaries to access and amend their data provided the request is legitimate and the request is made either directly by the person concerned or with their explicit authority. E.g. personal data should not be disclosed to an unauthorised person claiming to represent the individual, particularly if that data is of a sensitive nature
- Establish a complaints policy and procedure and respond promptly to any complaints or concerns beneficiaries may have about the use of their personal data.

Photo: Simon Rawles

[4] http://www.piafproject.eu/ref/A_step-by-step_guide_to_privacy_impact_assessment-19Apr2012.pdf
For more information please see: http://piafproject.eu/ref/PIAF_D3_final.pdf

ANNEXES: SUMMARY

ANNEX 1: MODEL PRIVACY IMPACT ASSESSMENT (PIA)

As stated in the document below: "The purpose of a PIA (Privacy Impact Assessment) is to demonstrate that programme managers and system owners have consciously incorporated privacy protections throughout the development life cycle of a system or programme. 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."

Additional approaches to identifying, managing and documenting risks to privacy exist. One such example is the Privacy Impact Assessment Framework (PIAF). PIAF is a European Commission co-funded project that aimed to encourage the EU and its Member States to adopt a progressive privacy impact assessment policy as a means of addressing needs and challenges related to privacy and to the processing of personal data.

The PIAF provides: ' *…a process that focuses on identifying the impacts on privacy of any new project, technology, service or programme and, in consultation with stakeholders, taking remedial actions to avoid or mitigate any risks. The process should start when a project is in the early planning stages, when there is still an opportunity to influence the project's design or outcome. The process should carry on throughout the project's life. New risks may emerge as the project progresses, and they should be assessed whenever they become apparent.*'

Wright D and Wadhwa K 2012 'A step by step guide to privacy impact assessment' [4]

ANNEX 2: MODEL CLAUSES FOR CONTRACTS WITH THIRD PARTIES

A: BENEFICIARY NOTICE AND CONSENT (PLAIN LANGUAGE TEMPLATE)

B: AID AGENCY AND E-TRANSFER SERVICE PROVIDER

Please note that the clauses represent a recommended standard but will need to be amended by the relevant Agency (i) to accommodate variations in terminology and naming conventions in the data protection laws applicable to the countries concerned; 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.

CaLP attempts to provide the practitioner with a starting point in the development of clauses that are in line with the Principles and Operational Standards outlined in this document.

Additional clauses will be made available on the CaLP website www.cashlearning.org

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