CHAPTER 9

CASH AND VOUCHER ASSISTANCE

Massimo Marelli

9.1 INTRODUCTION

Cash and Voucher Assistance[1] are a set of promising tools for supporting processes of survival and recovery from Humanitarian Emergencies. The terms Cash and Voucher Assistance, Cash Transfer Programming, cash-based interventions and cash-based assistance can be used interchangeably and are understood to encapsulate all types of cash transfers, i.e. both vouchers and cash, and all types of physical and digital delivery mechanisms.[2]

Cash transfers maximize the respect for affected people's choices and the trade-offs they face. The world of humanitarian response continues to use several different varieties of Cash and Voucher Assistance, ranging from vouchers that have to be exchanged for specific products or services from specific suppliers, to cash transfers that are made conditional on beneficiaries meeting some kind of requirement, or unrestricted and unconditional cash transfers that can be spent on anything affected people require.[3]

There are different forms of digitally delivered cash assistance, all of which is spent without restrictions, such as electronic cash (e-cash), which is a monetary value sent to people that can be spent digitally, or converted into hard cash (e.g. mobile money, pre-paid cards, bank transfers); and electronic vouchers, which are sent to people (through smart cards or mobile phones) that can be exchanged with approved merchants for approved items, with restrictions on spending possible.[4] Hard cash is sometimes also used, as well as paper vouchers.

It is widely recognized that the effectiveness and appropriateness of humanitarian aid provided through Cash and Voucher Assistance depends on the situation (e.g. can individuals obtain the items they need in a particular situation?).[5] Although some concerns have been raised about Cash and Voucher Assistance (e.g. inflation of the

1 Since the second edition of this Handbook, the terminology in the humanitarian sector has evolved: "Cash Transfer Programming" is more commonly referred to as "Cash and Voucher Assistance".

2 See Cash Learning Partnership (CaLP), "Cash Transfers Glossary", accessed 20 January 2022: www.humanitarianresponse.info/sites/www.humanitarianresponse.info/files/documents/files/calp-glossary_of_cash_transfer_programme_terminology.pdf.

3 The High Level Panel on Humanitarian Cash Transfers, "Doing Cash Differently: How Cash Transfers Can Transform Humanitarian Aid", Center For Global Development, London, 14 September 2015, 11: www.cgdev.org/publication/doing-cash-differently-how-cash-transfers-can-transform-humanitarian-aid.

4 European Commission, *10 common principles for multi-purpose cash-based assistance to respond to humanitarian needs*, March 2015: http://ec.europa.eu/echo/files/policies/sectoral/concept_paper_common_top_line_principles_en.pdf; European Commission, *The use of cash and vouchers in humanitarian crises*. DG ECHO Funding Guidelines, 11 March 2013: http://ec.europa.eu/echo/files/policies/sectoral/ECHO_Cash_Vouchers_Guidelines.pdf.

5 Paul Harvey and Sarah Bailey, "Cash Transfer Programming and the Humanitarian System", Background Note for the High Level Panel on Humanitarian Cash Transfers, Overseas Development Institute, London, March 2015: https://odi.org/en/publications/cash-transfer-programming-and-the-humanitarian-system.

local market), there is evidence supporting it as a "good value for money compared to in-kind alternatives".[6]

Research has shown that the greater use of humanitarian cash transfers where appropriate, without restrictions and delivered as electronic payments wherever possible, has benefits such as the following:[7]

- providing crisis-affected people with choice and greater control over their own lives;
- aligning the humanitarian system better with what people actually need;
- increasing the transparency of humanitarian aid and the prevention of fraud, by showing how much aid actually reaches the target population;
- increasing accountability of humanitarian aid, both to affected populations and to the tax-paying public in donor countries;
- potentially reducing the costs of delivering humanitarian aid to make limited budgets go further;
- supporting local markets, jobs and the incomes of local producers;
- increasing support for humanitarian aid from local people;
- increasing the speed and flexibility of humanitarian response;
- increasing financial inclusion by linking people with payment systems.

However, a number of difficulties and challenges also exist. Using Cash and Voucher Assistance in some Humanitarian Emergencies may not be an optimal solution (for example, in cases where the goods and services needed are not available, where local authorities oppose this type of humanitarian aid, or where the relevant market is at a risk of inflation).[8] Cash transfers are simply a tool to reach a programme objective, and so cash transfers are used as part of broader humanitarian assistance programmes, including measures providing protection, sanitation or health services.[9]

For Cash and Voucher Assistance to function, Humanitarian Organizations need to process individuals' Personal Data. This often includes data about an individual's or group's socioeconomic status and vulnerabilities. This poses inherent privacy-related threats and risks associated with the collection and handling of beneficiaries' Personal Data, in particular in light of the complex data flows they involve. Moreover, the use of digital technologies for Cash and Voucher Assistance often requires the involvement of non-humanitarian Third Parties (e.g. domestic and international mobile network providers, financial institutions and financial intelligence units). This means that Humanitarian Organizations lose control over the data collected and the metadata generated by the Cash and Voucher Assistance. These data can then be used for non-humanitarian purposes (e.g. to profile potential

6 Ibid.

7 The High Level Panel on Humanitarian Cash Transfers, *Doing Cash Differently*, 8.

8 Ibid., 11.

9 Ibid.

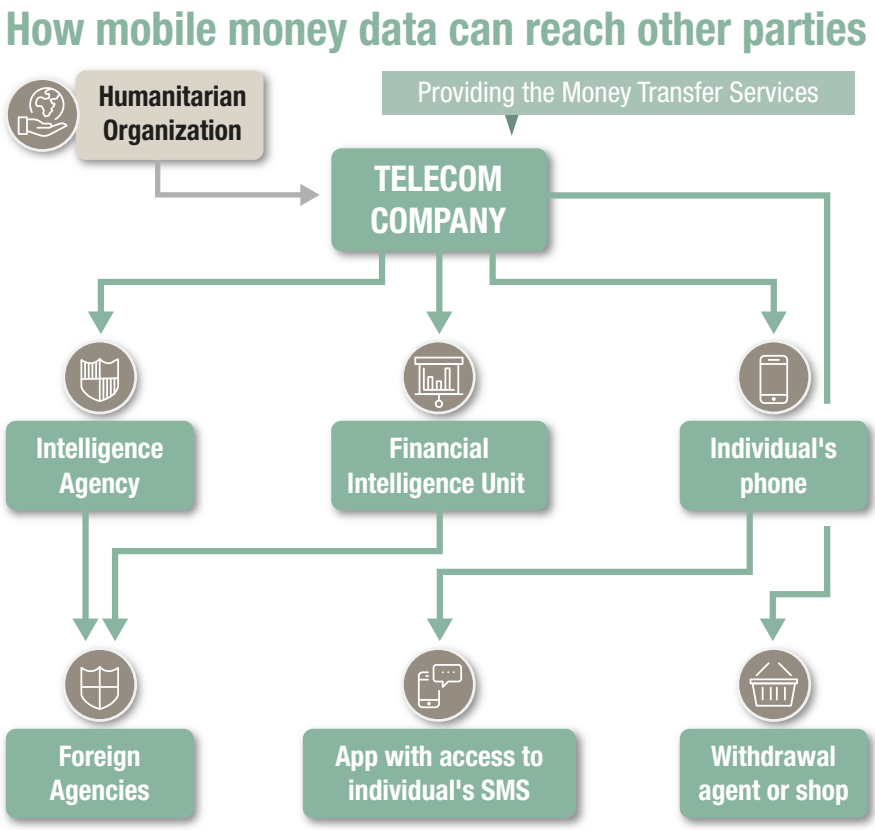

Figure 9.1. ICRC and Privacy International, chapter 6: Cash Transfer Programming, *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*, October 2018, p. 73.

customers). They can also be shared with external parties in order to comply with a legal obligation or under partnership agreements.[10]

In addition, a joint ICRC and Privacy International study stressed that, beyond knowingly collected and processed data, every single interaction generates what is known as metadata, i.e. data about data. These metadata are the inevitable result of the interaction with the system or service.

Finally, it is important to note that while the growing use of digital technology and connectivity is rendering previously "invisible" people "visible" to financial

10 ICRC and Privacy International, *The Humanitarian Metadata Problem: "Doing No Harm" in the Digital Era*, October 2018, chap. 6: www.icrc.org/en/download/file/85089/the_humanitarian_metadata_problem_-_icrc_and_privacy_international.pdf.

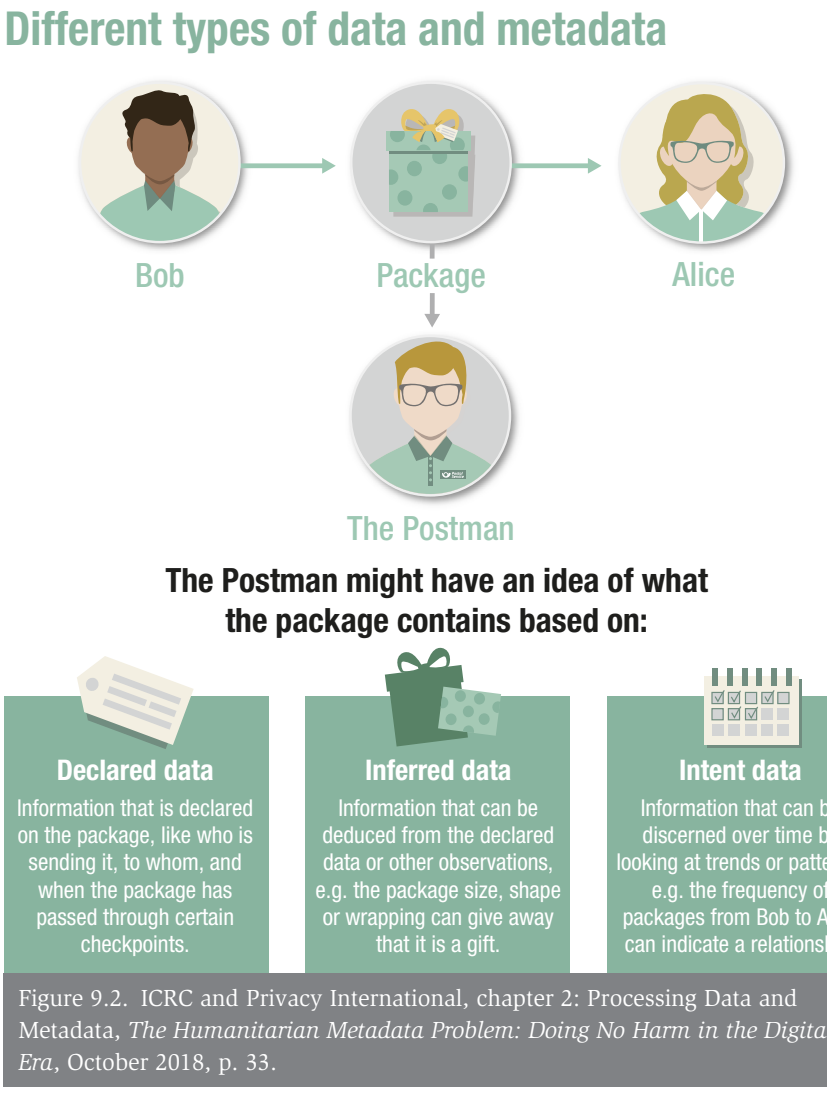

Figure 9.2. ICRC and Privacy International, chapter 2: Processing Data and Metadata, *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*, October 2018, p. 33.

institutions, these digital identities and footprints can help to include people who were overlooked under previous programmes. However, this new visibility can also expose affected people to risks.[11] The mere fact that they are seeking assistance from

11 For a longer exploration of this, see Jo Burton, "'Doing no harm' in the Digital Age: What the digitalization of cash means for humanitarian action", *International Review of the Red Cross*, Vol. 102, No. 913, April 2020, pp. 43–73: https://doi.org/10.1017/S1816383120000491. The advantages and disadvantages of "making the invisible visible" were discussed during the DigitHarium months on Digitalized Assistance and Digital identities. See: ICRC, "DigitHarium Month #2: Digitalized Assistance, Social Protection and Humanitarian Data Concerns", International Committee of the Red Cross,

a Humanitarian Organization can reveal their affiliation with a particular group and expose them to discrimination. In other words, the inevitable visibility created by digital engagement can pose a threat in humanitarian situations. Digital visibility and profiling can become an instrument for financial discrimination, running counter to the original purpose of the Cash and Voucher Assistance.[12]

9.2 APPLICATION OF BASIC DATA PROTECTION PRINCIPLES

The inherent privacy-related threats and risks associated with the collection and handling of beneficiaries' Personal Data for Cash and Voucher Assistance can arise from inadequate organizational and technical data security measures. Humanitarian Organizations should also consider the long-term impact of the data generated, directly or indirectly, by Cash and Voucher Assistance. As Cash and Voucher Assistance makes use of existing services and systems including banks and telecommunications operators, Humanitarian Organizations may be required to collect data from affected people in order to comply with Know Your Customer,[13] SIM card registration[14] and other obligations to which such bodies are subject. Personal Data collected for Cash and Voucher Assistance can involve a variety of data sets that may not have been necessary for other types of humanitarian aid.[15] These data are shared with private entities to enable the distribution of financial aid.

Furthermore, careful consideration needs to be given not just to the data collected but also to the data generated, i.e. to the metadata produced through the practical arrangements of Cash and Voucher Assistance. Different legal and regulatory obligations apply to the collection, sharing and retention of such data. For example, in the case of mobile money, this includes data such as: the sender's and recipient's phone numbers; the date and time of the financial transaction; the transaction ID; the location and size of the transaction; the store where it was conducted; and any

9 March 2021: www.icrc.org/en/digitharium/digitharium-month-2; ICRC, "DigitHarium Month #9: Digital Identities and Humanitarian Operations", International Committee of the Red Cross, 18 February 2022: www.icrc.org/en/digitharium/digitharium-month-9.

12 ICRC and Privacy International, *The Humanitarian Metadata Problem*, 68–69.

13 Know Your Customer (KYC) is a process by which businesses check the identity of their customers in order to comply with anti-money laundering and anti-corruption regulations and legislation.

14 Kevin P. Donovan and Aaron K. Martin, "The rise of African SIM registration: The emerging dynamics of regulatory change", *First Monday*, Vol. 19, No. 2, 26 January 2014, sec. IV: https://doi.org/10.5210/fm.v19i2.4351.

15 Cash Learning Partnership (CaLP), "Protecting Beneficiary Privacy, Principles and Operational Standards for the Secure Use of Personal Data in Cash and e-Transfer Programmes", 2020, 4: www.calpnetwork.org/wp-content/uploads/2020/01/calp-beneficiary-privacy-web.pdf.

agents involved at either end. Such data can be used to infer other information and intelligence, which could be used to profile, target and monitor users.[16] Humanitarian Organizations must therefore be aware of the ways in which data can be used to infer information about their beneficiaries' behaviours, movements, affiliations and other characteristics. The ability to draw inferences about affected people is possible long after the programme ends.

With an increasing number of Humanitarian Organizations opting for Cash and Voucher Assistance to provide aid, there is a pressing need to consider the impact (e.g. will individuals receiving financial aid be subject to discrimination?) and measures mitigating the risks associated with the Personal Data Processing needed to distribute this type of aid.[17]

Data protection issues result from the fact that data are collected, stored and cross-matched by Data Controllers or Data Processors during cash assistance operations. Often, the data collected during Cash and Voucher Assistance relates to socioeconomic factors and vulnerabilities. The data are used to target assistance, either for a subset of the affected people (for needs assessment research), or for a wider group, potentially including people who do not ultimately receive cash transfers. For all recipients, the Personal Data collected during the process typically include the following: name, surname, mobile phone number, "Know Your Customer"[18] data, geolocation/other phone metadata and Biometrics. Humanitarian Organizations may also collect data related to socioeconomic factors or vulnerabilities for the purposes of targeting assistance. These data, once collected and stored, may enable Processing for other purposes and/or other types of data Processing, such as Data Analytics or data mining.[19]

The complexity of the flow of data between Humanitarian Organizations and partner organizations using Cash and Voucher Assistance also gives rise to data protection issues, which are dealt with in Section 9.5 – Data sharing.

9.3 BASIC PRINCIPLES OF DATA PROTECTION

The basic principles of data protection constitute the baseline to be respected while engaging in any type of Personal Data Processing. These include the principle of the

16 ICRC and Privacy International, *The Humanitarian Metadata Problem*, 73–75.

17 Ibid., 4.

18 See Glossary.

19 See Chapter 17: Artificial Intelligence, and particularly Section 17.1.2 – Artificial Intelligence in the humanitarian sector.

fairness and lawfulness of the Processing, the principle of transparency, the purpose limitation principle, the data minimization principle and the data quality principle.[20]

The data protection discussion in this chapter builds on the principles set out in Part I, which examines them in greater detail.

9.3.1 LEGAL BASES FOR PERSONAL DATA PROCESSING

Humanitarian Organizations may process Personal Data using one or more of the following legal bases:

- the vital interest of the Data Subject or of another person;
- the public interest, in particular based on an organization's mandate under national or international law;
- Consent;
- a legitimate interest of the organization;
- the performance of a contract;
- compliance with a legal obligation.

Obtaining the valid informed Consent[21] of beneficiaries in programmes using Cash and Voucher Assistance can be challenging, due to the amount and complexity of information that would need to be provided to ensure that the beneficiaries fully appreciate the risks and benefits of Processing. Moreover, merely interacting with the service inevitably generates metadata without the user's say.[22] As with other cases when Personal Data are collected as a prerequisite for assistance to be provided to affected people, unless an alternative method of providing assistance is also made available, it can be argued that an individual in need of assistance has no real choice as to whether to give Consent or not and, accordingly, Consent may not be considered valid. If Consent is not possible, then another legal basis should be used, as set out below.

Regardless of the legal basis selected, and following the principle of transparency, beneficiaries should at least be informed individually or collectively as to the nature of the programme being provided, the legal basis for Processing, what data are being collected, by whom and why, whether providing the data is mandatory or voluntary, the sources of the data, how long it will be stored for, which Data Processors are involved, who else the data will be shared with, and their rights (including the right to redress).

Humanitarian Organizations should:[23]

- aspire to obtain the active and informed Consent of beneficiaries for the use of their Personal Data when using Cash and Voucher Assistance.

20 See also Chapter 2: Basic principles of data protection.

21 See Section 3.2 – Consent.

22 ICRC and Privacy International, *The Humanitarian Metadata Problem*. 21.

23 CaLP, "Protecting Beneficiary Privacy", 14.

- only use alternatives to active and informed Consent where obtaining it is impractical or valid Consent cannot be obtained for other reasons set out herein. Legitimate reasons for not seeking active and informed Consent include urgency, or if the circumstances of the distribution make "active and informed Consent" meaningless.
- if possible, ensure that valid Consent can be provided or offer an alternative method of assistance for the individuals who are not comfortable with the data flows and/or stakeholders involved in the use of Cash and Voucher Assistance.
- to the best of their knowledge given publicly available information, inform beneficiaries about the data and metadata which may be generated, collected and processed by Third Parties whose services and systems the Humanitarian Organization is using (including KYC for banks and SIM card registration by telecommunications operators).

In light of the potential effectiveness of cash-based operations in disaster and emergency conditions and the rapidity of deployment if properly prepared in advance (e.g. if compared to in-kind assistance), the vital interests of the Data Subject or another person might constitute a plausible alternative legal basis for the relevant Processing when Humanitarian Organizations are unable to obtain the individuals' Consent. However, as always with this legal basis and as set out elsewhere in this Handbook, its use should be carefully considered.

Public interest could constitute a suitable legal basis for Processing data in the use of Cash and Voucher Assistance where a mandate to carry out Humanitarian Action is established in national, regional or international law and where no Consent is obtained and no vital interests are triggered, as per the cases discussed above.

Humanitarian Organizations may also process Personal Data where this is in their legitimate interest, provided that this interest is not overridden by the fundamental rights and freedoms of the Data Subject. Such legitimate interests may include making humanitarian aid delivery more effective and efficient, preventing fraud and duplication of aid.

9.3.2 PURPOSE LIMITATION AND FURTHER PROCESSING

At the time of data collection, the Humanitarian Organization concerned must determine and set out the specific purpose(s) for which data are processed.[24] The specific purpose(s) should be explicit and legitimate and, in the case of Cash and Voucher Assistance, should involve the provision of assistance to enable affected people to access the goods and services they need.

The purposes of the Processing need to be clarified and communicated to individuals at the time of collection.

24 See Section 9.3.1 – Legal bases for Personal Data Processing.

Personal Data may be processed for purposes other than those initially specified at the time of collection where the Further Processing is compatible with those purposes, including where the Processing is necessary for historical, statistical or scientific purposes. In order to establish whether Further Processing is compatible with the purpose for which the data were initially collected, attention should be paid to the following factors:

- any link between the purposes for which the data were initially collected and the purposes of the intended Further Processing;
- the situation in which the Personal Data were collected, in particular, the relationship between Data Subjects and the Data Controller, as well as the relationship with the Data Processor;
- the nature of the Personal Data;
- the possible consequences of the intended Further Processing for Data Subjects;
- the existence of appropriate safeguards;
- the reasonable expectation of the Data Subjects as to possible further uses of the data.

When assessing the above, the humanitarian purposes of the data Processing should be given particular consideration.

Additional purposes that may be involved in the Processing by or of interest to commercial processors (e.g. financial institutions and mobile phone operators) should also be considered. This may potentially include: cross-checking lists of beneficiaries against lists of designated persons; retention of metadata for law enforcement purposes; profiling beneficiaries for creditworthiness, etc.[25] The following consequences could occur should commercial Data Processors be obliged or in a position to process Personal Data for purposes other than the exclusively humanitarian purpose envisaged:

- It would become questionable whether the entities in question are indeed Data Processors, and not new Data Controllers, deciding on the means and purposes of Processing.
- The additional Processing may be incompatible with the initial purpose for collection and require a new legal basis. While a new legal basis may perhaps be found (such as compliance with a legal obligation to report designated persons), Humanitarian Organizations should carefully consider whether this is compatible with the Neutral, Impartial and Independent nature of Humanitarian Action.

Contractual clauses in the Processing agreement should restrict Further Processing by Data Processors as much as possible.

In the case of Cash and Voucher Assistance, Humanitarian Organizations should be aware of the data and metadata processed by Data Processors whose services and

25 ICRC and Privacy International, *The Humanitarian Metadata Problem*, chap. 6.

systems they are using. These should be included in the DPIA to identify any areas that need to be regulated through contractual clauses.[26]

EXAMPLE:
In the case of a system set up to disburse cash or voucher assistance by a Humanitarian Organization, to which purpose the individuals concerned have consented, the same system cannot be used to transmit participants' data to donors of the Humanitarian Organization for cross-referencing purposes.

Likewise, any data collected cannot be used by a financial institution to assess a beneficiary's creditworthiness and eligibility for financial services, including after they have received aid from a Humanitarian Organization.

9.3.3 DATA MINIMIZATION

The information collected for the purposes of cash assistance operations needs to be proportionate to these purposes. That is, only the Personal Data necessary for the identification of individuals should be collected and processed and any "excess" information that is not relevant to the Cash and Voucher Assistance purposes should not be collected and, if collected, should be deleted.

Given that many types of data are collected when using Cash and Voucher Assistance, compartmentalization of the data is recommended as a way to meet data minimization requirements, with access being provided on a need-to-know basis. Additionally, contractual provisions could be provided against the Further Processing by commercial entities.

In assessing the application of the data minimization principle, it is also important to take into account the data generated as part of the Cash and Voucher Assistance by Data Processors, such as credit transaction metadata and mobile network metadata.

One possible option in programmes using Cash and Voucher Assistance is for the Humanitarian Organization, once the individual is identified, to only transfer to the commercial service provider (e.g. bank or mobile network operator), when feasible, a unique identifier (from which the receiving entity cannot identify the final beneficiary) and the amount of cash to be distributed, so as to limit the risks to the individuals concerned. However, it is important to consider the limitations of these approaches, since programmes such as these depend on rigid systems provided by financial institutions, telecommunications operators and other relevant organizations. Likewise, it is important to recognize the limitations of current Pseudonymization (or imperfect

26 For more consideration about DPIAs, see Section 9.8 – Data Protection Impact Assessments

Anonymization) techniques and the implications for Reidentification, especially when data can be correlated with other sources to enable Reidentification.[27]

9.3.4 DATA RETENTION

Humanitarian Organizations are advised to ensure that beneficiary data are not held (whether by them or by Third Party Data Processors) for longer than is required to fulfil the specific purposes for which they were collected, unless retention is potentially useful for repeat distributions. The Personal Data of beneficiaries who have left the programme should be deleted by the organization, its Data Processors, and any Third Parties that have had access to the data. The Humanitarian Organization should verify data deletion by the commercial service provider, as far as this is possible. Any information that is deemed necessary to keep at the end of a programme should only be kept if it is related to data for which there is a legitimate purpose, such as possible future programmes, auditing or reporting purposes, monitoring and evaluation. Ideally, and to the extent that this is meaningful, data retained for these reasons should be aggregated and/or anonymized.

In considering data retention, Humanitarian Organizations should also consider the retention obligations that may apply by virtue of domestic law to some Data Processors, such as financial institutions, credit card companies and mobile phone network operators. These should be included in programme DPIAs and privacy policies.

9.3.5 DATA SECURITY

In order to avoid potential misuse of the Personal Data collected and processed during Cash and Voucher Assistance, it is essential that adequate and proportionate security measures are implemented. Humanitarian Organizations are advised to implement appropriate technical and operational security standards for each stage of the collection, use and transfer of beneficiary data, and processes should be put in place for the protection of beneficiary Personal Data from loss, theft, damage or destruction; this includes backup systems and effective means to respond to security breaches and prevent unauthorized access, disclosure or loss.[28]

It is also advisable for the Humanitarian Organizations to protect "by design" the Personal Data they obtain from beneficiaries either for their own use or for use by Third Parties for each programme using cash or vouchers that they initiate or implement. This means that they should build privacy protections into the processes

27 Larry Hardesty, "How Hard Is It to 'de-Anonymize' Cellphone Data?". MIT News | Massachusetts Institute of Technology (blog), 27 March 2013: https://news.mit.edu/2013/how-hard-it-de-anonymize-cellphone-data. See also Section 2.3 – Aggregate, Pseudonymized and Anonymized data sets.

28 See Section 2.8 – Data security and Processing security.

and mechanisms they use to implement Cash and Voucher Assistance. Encryption or compartmentalization of information can be viable solutions to meet this need.

Humanitarian Organizations must take steps to inform themselves about the measures taken by potential Data Processors and other Third Parties on whose systems, services and infrastructure they rely prior to contracting them. Personal Data, at rest and in transit, as well as the infrastructure relied upon for Processing, should be protected by security safeguards against risks such as unlawful or unauthorized access, use and disclosure, as well as loss, destruction or damage of data. As part of their due diligence and DPIAs, Humanitarian Organizations should inform themselves about any publicly known security incidents experienced by Data Processors and other Third Parties on whose systems, services and infrastructure they rely, and what measures they have subsequently put in place to ensure the security and integrity of the data, at rest and in transit, and the infrastructure relied upon.

Data storage and potential International Data Sharing also need to be taken into consideration. For example, for refugees, there may be serious data protection risks associated with using a regional bank that has a branch or storage facility in the country of origin of the refugees, as the data may be requested by national authorities.

When selecting external Data Processors, the security measures they can guarantee should be a key factor.

9.4 RIGHTS OF DATA SUBJECTS

The right to information should be respected by ensuring that beneficiaries are informed individually or collectively as to the nature of the programme being provided, what information is being collected, by whom and why, and which Data Processors are involved. Humanitarian Organizations should be transparent about how they intend to use the Personal Data they collect and process. They should provide privacy notices accounting for the full data flow and data retention envisaged to beneficiaries who want more detailed information.

Adequate infrastructure and resources should be put in place to facilitate the rights to access, objection, deletion and rectification with regard to any programme using Cash and Voucher Assistance. In this respect, it is advisable to incorporate complaint procedures into Personal Data Processing practices and internal data protection policies.

9.5 DATA SHARING

Personal Data Processing for Cash and Voucher Assistance may include data sharing with Data Processors and Third Parties when the datasets have been collected and

processed by different Data Controllers or Data Processors (for example, if Humanitarian Organizations implementing a cash assistance programming system outsource individual identification in the field to on-site operators). It is important to take into consideration data protection requirements before sharing data and to note that 'sharing' includes not only situations where data are actively transferred to Third Parties, but also those when they are made accessible to others (e.g. sharing a database which contains beneficiaries' Personal Data).

Humanitarian Organizations may rely on partner organizations to collect data on their behalf, or on commercial organizations (such as financial institutions and mobile operators) involved in carrying out such programmes. These other organizations may be subject to a variety of legal and organizational requirements that lead them to share data with Third Parties (including regulators), which can include the following:

- "Know Your Customer" (KYC) obligations requiring the collection of more Personal Data than is strictly necessary for the purposes of providing assistance.
- obligations to cross-check KYC information against lists of designated persons established by local authorities, including entities potentially involved in a conflict or situation of violence. This process may potentially be monitored by public authorities, and may involve reporting obligations. This in turn gives rise to questions as to inclusion (i.e. can beneficiaries be excluded from an assistance programme on the basis of a match being found) and compromises the neutrality and independence of Humanitarian Action.
- collection of additional data as part of the process, such as geolocation or unique telephone identifiers and other mobile network metadata, when mobile phone operators are involved;
- requirements for SIM card registration;
- retention obligations incompatible with the information provided by Humanitarian Organizations at the time of collection;
- additional commercial purposes, such as profiling individuals for creditworthiness or advertising;
- additional obligations imposed on them by national law.

Privileges and immunities are also of great significance with respect to Cash and Voucher Assistance. In this regard, the provisions of Section 10.9 – Privileges and immunities and the cloud should be considered for Cash and Voucher Assistance.

9.6 INTERNATIONAL DATA SHARING

Data protection law restricts International Data Sharing, so Humanitarian Organizations should have mechanisms in place to provide a legal basis for it in Cash and Voucher Assistance, as discussed in Chapter 4: International Data Sharing.

Humanitarian Organizations should examine whether International Data Sharing has a legal basis under applicable law and their own internal policies before carrying it out.

Financial services are highly interconnected in a way that Humanitarian Organizations cannot control. The way in which data might travel within and outside national borders is affected by this interconnectedness, as well as by national laws, regulations and practices. For this reason, Humanitarian Organizations must discuss, with all institutions involved in the Cash and Voucher Assistance: (i) who their main partners are, nationally and internationally, and (ii) whether Cash and Voucher Assistance data can be kept outside any information exchanges.[29]

9.7 DATA CONTROLLER/DATA PROCESSOR RELATIONSHIP

The use of Cash and Voucher Assistance by a Humanitarian Organization may involve local or international commercial service providers for project implementation. Humanitarian Organizations may also cooperate among themselves in sharing databases of the information collected via these operations. It is thus crucial to determine which parties actually determine the purposes and means of data Processing (and thus are Data Controllers), and which merely take instructions from Data Controllers (and thus are Data Processors). It is also possible that multiple parties might be considered to be joint Data Controllers. When the roles have been clearly defined and the corresponding tasks assigned, data sharing across Humanitarian Organizations and/or national borders and/or third (private or state) bodies should generally be covered by appropriate contractual arrangements.

It should be remembered that although Personal Data may be protected while kept in the systems of Humanitarian Organizations which benefit from privileges and immunities under international law, the same data may lose such protection when transferred to Data Processors not enjoying those privileges and immunities. In addition, Data Processors may be obliged by local legislation to share data with government agencies and may even be obliged not to tell the Humanitarian Organizations from which the data originated about this data sharing.

9.8 DATA PROTECTION IMPACT ASSESSMENTS

Data Protection Impact Assessments (DPIAs) need to be drafted and tailored to each programme utilizing cash and vouchers. Cash and Voucher Assistance may differ not

29 ICRC and Privacy International, *The Humanitarian Metadata Problem*, 79.

only from organization to organization, but also within an organization itself. Each programme constitutes a separate data protection activity which should be subject to a DPIA. DPIAs will help the Humanitarian Organization to (a) identify the privacy risks to individuals, in particular, those deriving from the data flow and stakeholders involved; (b) identify the privacy and data protection compliance liabilities for the organization; (c) protect the organization's reputation and instil public confidence in the programme; and (d) ensure that the organization does not compromise on the neutrality of its Humanitarian Action.

It is recommended that Humanitarian Organizations analyse, document and understand the flow of beneficiary data for each programme they initiate or implement internally within their own organization or externally with others, identify the risks involved and develop risk mitigation strategies. Particular issues often associated with commercial service providers and relating to KYC regulations, mandatory reporting to national authorities, International Data Sharing and potential cloud storage, need to be specifically assessed and weighed against the benefits of using Cash and Voucher Assistance.

A template DPIA for Cash and Voucher Assistance has been developed by the Cash Learning Partnership.[30]

30 CaLP, "Protecting Beneficiary Privacy", 18.