OCHA centre for humdata

THE CENTRE FOR HUMANITARIAN DATA

GUIDANCE NOTE SERIES
DATA RESPONSIBILITY IN HUMANITARIAN ACTION

DATA RESPONSIBILITY IN CASH AND VOUCHER ASSISTANCE

KEY TAKEAWAYS:

- Humanitarian actors have made considerable progress in promoting data responsibility in cash and voucher assistance (CVA) in recent years. However, gaps remain between global frameworks for data responsibility and their practical application in the delivery of CVA.
- There are many resources available on data protection in CVA programmes, but guidance and practical tools are lacking for the responsible management of sensitive non-personal data.
- Common data-related benefits in CVA include: (i) improved understanding of beneficiary priorities, needs and preferences; (ii) improved targeting of assistance, including deduplication of beneficiary lists; (iii) increased efficiency and effectiveness of different delivery mechanisms; and (iv) enhanced transparency and accountability.
- Common data-related risks in CVA include: (i) exposure of sensitive data that could lead to various forms of harm for affected people and/or humanitarian staff; (ii) breaches in data protection, data privacy and data security; (iii) potential misuse of data for non-humanitarian purposes by third parties; and (iv) loss of trust between affected people and humanitarian organizations.
- Humanitarian organizations can improve data responsibility in CVA by taking the following actions: (i) mapping the CVA data ecosystem; (ii) establishing an information sharing protocol specific to CVA programmes; (iii) establishing data sharing agreements for the exchange of personal data; (iv) conducting data impact assessments for all CVA interventions; (v) introducing data incident management procedures; and (vi) tracking issues and progress on data responsibility in CVA through coordination structures.

INTRODUCTION

As digital tools become more central in the delivery of cash and voucher assistance (CVA), humanitarian organizations, financial service providers, and other stakeholders gather, store, use and share increasingly large volumes of data. These trends have been accelerated in the response to COVID-19, for which cash actors have scaled up and adapted their CVA programmes in line with the particular challenges posed by the pandemic, with a preference towards contactless electronic or mobile payments to reduce the risk of transmission.[1]

[1] Guidance note on the role of Cash and Voucher Assistance to reduce financial barriers in the response to the COVID-19 pandemic, in countries targeted by the Global Humanitarian Response Plan COVID-19.

According to the 2020 State of the World's Cash report, perceptions of digital and data management risks have also increased in prominence in recent years.[2] The following concerns have been acknowledged in various CVA fora[3]: (i) there is a significant gap in practical resources to help practitioners marry the ethical standards contained in data responsibility policies with the day-to-day pressure to deliver programmes; (ii) there are no mechanisms in place to enable collective sharing of, and learning from, critical data incident management cases; and (iii) lower risk appetite in CVA, partially due to Anti-Money-Laundering/ Counter-Terrorism measures and the political economy of cash, which extends into the data management space.

Humanitarian actors have made considerable progress in promoting data responsibility in CVA. A range of initiatives[4] aim to ensure the protection of aid recipients and support more efficient, collaborative and data-driven ways of working. Bilateral and multilateral engagements between humanitarian organizations, including global data sharing agreements and joint programme delivery strategies, complement these collective efforts.

Nevertheless, gaps remain between global frameworks for data responsibility and their practical application in the delivery of CVA. This guidance note aims to help fill these gaps by offering an overview of the common data-related benefits and risks encountered by cash actors. It provides a set of actions that organizations can take to improve data responsibility in the delivery of cash and voucher assistance.

DATA MANAGEMENT FOR CASH AND VOUCHER ASSISTANCE

CVA requires the collection of personal and non-personal data that would be considered sensitive in most humanitarian settings. Personal data commonly collected in CVA programmes includes national ID numbers, phone numbers and addresses, family members' names, personal bank details, and biometric data, among others. Common non-personal data in CVA programmes includes microdata from surveys and needs assessments, demographically identifiable information about different groups receiving assistance, location data for CVA distribution points, and anonymized and/or aggregated community feedback data, among others. The delivery of CVA also generates new forms of metadata[5] that humanitarian organizations previously have not had to manage, such as data about transactions with different financial service providers and affected populations' spending or consumption patterns.

Unlike other areas of humanitarian assistance, CVA involves a particularly wide and diverse range of actors. The complexity of the flow of data between humanitarian organizations and different partners involved in the delivery of CVA gives rise to data protection issues and other concerns, outlined in more detail below.

Different standards for data responsibility are applied in CVA programmes across organizations and contexts. This is due to (i) varying levels of familiarity with existing data responsibility guidance and related capacity gaps among programme staff and (ii) evolving data risks related to new delivery mechanisms and partnership models for CVA. Existing guidance[6] is primarily focused on the safe management and protection of personal data, and does not fully address concerns related to non-personal data that is sensitive in many contexts and requires robust protections.

[2] CaLP, 2020. **State of the World's Cash Report 2020**.

[3] *Ibid.*

[4] These include efforts through the Grand Bargain Cash workstream working group on Cash and Risk, the Cash Learning Partnership (CaLP), the Common Cash Delivery Network, and the UN Common Cash Statement, among others.

[5] International Committee of the Red Cross (ICRC) and Privacy International, 2018. **The humanitarian metadata problem: "Doing no harm" in the digital era**.

[6] For more on data protection in cash and voucher assistance, see CaLP's **Protecting Beneficiary Privacy**, the Common Cash Delivery (CCD) Network's **Protecting personal data and privacy in field work: A guide for data sharing between humanitarian organizations**, and the ICRC **Handbook on Data Protection in Humanitarian Action**.

Know Your Customer (KYC) regulations

Know Your Customer regulations, also known as customer due diligence, are designed to combat money laundering, terrorist financing and other related threats to the financial system. They refer to the ID checks that financial institutions perform to comply with national financial regulations. While some humanitarian agencies are not directly subject to KYC regulations, the financial service providers that they partner with are. As such, these regulations have a direct impact on the responsible management of data generated and shared for cash and voucher assistance. KYC requirements are set at the national level and may vary depending upon specific criteria.

For more on KYC in humanitarian cash and voucher assistance, see ***elan's Tip Sheet on KYC Regulations*** and ***UNHCR and World Vision's Know Your Customer Standards and Privacy Recommendations for Cash Transfers***.

DATA-RELATED BENEFITS AND RISKS IN CASH AND VOUCHER ASSISTANCE

Data responsibility requires a clear understanding of both the benefits and the risks associated with data management. While they may vary from one setting to the next, there are commonly recognized data-related benefits and risks within the CVA community.

Benefits in CVA include:

- Improved understanding of beneficiary priorities, needs and preferences.
- Improved targeting of assistance, including deduplication of beneficiary lists.
- Increased efficiency and effectiveness of different delivery mechanisms.
- Enhanced transparency and accountability.

Risks in CVA include:

- Exposure of sensitive data that could lead to various forms of harm for affected people and/or humanitarian staff.
- Breaches in data protection, data privacy and data security.
- Potential misuse of data for non-humanitarian purposes by third parties.
- Loss of trust between affected people and humanitarian organizations.

Practical Guidance for the Cash Community: CaLP's Data Responsibility Toolkit

CaLP's ***Data Responsibility Toolkit*** offers detailed guidance on data responsibility in cash and voucher assistance. The toolkit aims to better reflect the complexity of partner relations, operational delivery models and associated data flows. It also aims to address elements of remote data collection that emerged in early 2020 in light of COVID-19.

The toolkit highlights the need for an ecosystem approach and power analysis among those who collect, use and share data from CVA recipients. It also notes the need for contextualization, creativity, capacity and collaboration among CVA actors and across organizational teams to ensure better protection of data.

The toolkit includes in-depth consideration of some of the tensions among different actors with regard to data, as well as orientation on data sharing, relationships between data controllers and data processors, privacy impact assessments, lawful bases for data collection (including consent and legitimate interests), preparing for possible critical data incidents or breaches, and communication with affected populations about data collection and processing.

It is structured around the different steps of a data lifecycle typical to CVA programmes and covers both personal and non-personal data, while also incorporating new legal requirements stemming from the European Union's General Data Protection Regulation.

RECOMMENDATIONS FOR IMPROVING DATA RESPONSIBILITY IN CASH AND VOUCHER ASSISTANCE

Data responsibility requires the implementation of principled actions at different levels of a humanitarian response. This includes actions to ensure data protection and data security, as well as strategies to minimize risks while maximizing benefits of data management.

The Centre for Humanitarian Data ('the Centre'), CaLP and NORCAP/Norwegian Refugee Council recommend following actions to improve data responsibility in the delivery of cash and voucher assistance:

- **Map the CVA data ecosystem**
- **Establish an information sharing protocol specific to CVA programmes**
- **Establish data sharing agreements for the exchange of personal data**
- **Conduct data impact assessments for all CVA interventions**
- **Introduce data incident management procedures**
- **Track issues and progress on data responsibility in CVA through coordination structures**

The table below provides a description of these actions and references to additional guidance and templates from different humanitarian organizations where available.

Action	Description
Map the CVA data ecosystem	A data ecosystem map helps identify data gaps and possible duplications, and enables prioritization and strategic decision-making on responsible data management. It provides a summary of major data management activities, including the scale, scope and types of data being processed, the stakeholders involved, the data flows between different actors, and processes and platforms in use in the delivery of CVA in a given context. The data ecosystem mapping exercise should be completed and subsequently updated on an annual basis by the Cash Working Group (CWG) in collaboration with their partners.
Establish an information sharing protocol specific to CVA programming	An information sharing protocol (ISP) serves as the foundation for a collective approach to responsible data and information exchange. The ISP sets out terms that all humanitarian organizations and third-party service providers involved in delivering CVA agree to uphold. It should complement any pre-existing bilateral data sharing agreements (see below), align with applicable Know Your Customer (KYC) standards, and include key elements such as a data sensitivity classification and a data retention and destruction schedule. An ISP may also specify a minimum core dataset[7] to facilitate the provision of cash assistance in a particular context. A template ISP[8] is included in the OCHA Data Responsibility Guidelines. The development of an ISP specific to CVA programming should be completed as a collective exercise led by the CWG.
Establish data sharing agreements	A data sharing agreement (DSA) establishes the terms and conditions that govern the sharing of personal data. It is primarily used for data sharing between two parties and is typically established at the country level. In accordance with data protection frameworks, signing a DSA is required for the sharing of personal data. In CVA programmes, DSAs or similar agreements are required not only between humanitarian organizations and their partners but also with FSPs and other third parties involved in the delivery of assistance.

[7] See for example the **Minimum Core Assistance Delivery Dataset for Affected Populations**.

[8] OCHA, 2019. **Working Draft Data Responsibility Guidelines**, 55-62.

Conduct data impact assessments for all CVA interventions	Data impact assessments[9] determine the expected risks, harms and benefits, as well as privacy, data protection and/or human rights impacts of a data management activity. An assessment informs the design and implementation of data management activities in a way that maximizes benefits and minimizes risks. The most common type of data impact assessment in CVA programmes is a Data Protection Impact Assessment, which focuses explicitly on personal data. If a CVA programme also generates large volumes of non-personal data, organizations should try to expand on their standard assessment template to also address risks, harms and benefits related to non-personal data.
Introduce data incident management procedures	Managing, tracking and communicating about data incidents requires standard operating procedures for incident management[10] and a central registry or log that captures key details about the nature, severity, and resolution of each incident. This will often include a mechanism for rectification and redress through which beneficiaries can seek resolution of issues related to the provision of CVA, including concerns about the management of their data. While organizations are encouraged to establish their own data incident management procedures, collective monitoring of incidents and sharing of lessons learned via the CWG is important in the complex and interconnected CVA data ecosystem.
Track issues and progress on data responsibility in CVA through coordination structures	Coordination structures such as a Cash Working Group can serve as a common platform for monitoring collective progress and/or challenges and opportunities for data responsibility. They can also support improved coordination and decision-making to advance data responsibility in CVA delivery in a given context.

Organizations are encouraged to share their experience in promoting data responsibility in the delivery of cash and voucher assistance with the Centre via centrehumdata@un.org.

COLLABORATORS: **CALP AND NORCAP/NORWEGIAN REFUGEE COUNCIL.**

The Centre for Humanitarian Data ('the Center'), together with key partners, is publishing a series of eight guidance notes on Data Responsibility in Humanitarian Action over the course of 2019 and 2020. The Guidance Note series follows the publication of the OCHA Data Responsibility Guidelines in March 2019. Through the series, the Centre aims to provide additional guidance on specific issues, processes and tools for data responsibility in practice. This series is made possible with the generous support of the Directorate-General for European Civil Protection and Humanitarian Aid Operations (DG ECHO).

This project is co-funded by the European Union

This document covers humanitarian aid activities implemented with the financial assistance of the European Union. The views expressed herein should not be taken, in any way, to reflect the official opinion of the European Union, and the European Commission is not responsible for any use that may be made of the information it contains.

[9] This includes Data Protection Impact Assessments as well as other types of assessments that consider the potential risks, harms, and benefits of a data management exercise. Learn more in this **Guidance Note on Data Impact Assessments** by the Centre for Humanitarian Data, ICRC, Privacy International, and UN Global Pulse.

[10] Learn more in this **Guidance Note on Data Incident Management** by the Centre for Humanitarian Data and the Jackson Institute for Global Affairs at Yale University.