The Cash Learning Partnership

DATA RESPONSIBILITY TOOLKIT

A GUIDE FOR CASH AND VOUCHER PRACTITIONERS

TABLE OF CONTENTS AND ACKNOWLEDGEMENTS

CONTENTS

ACKNOWLEDGEMENTS

The Data Responsibility Toolkit – A guide for Cash and Voucher Practitioners was commissioned by CaLP with funding from the German Federal Foreign Office.

The research for this publication was conducted between June and September 2020 by Linda Raftree, an independent consultant.

The publication was developed by Linda Raftree, with editorial and content supervision and support from Anna Kondakhchyan of CaLP. This is a collaborative piece of work, with invaluable input from the many organisations and CVA practitioners who have generously contributed their ideas and time to the research process through the key informant interviews and data sources.

Our particular thanks go to the Advisory Committee members for their critical support in guiding the development of the Toolkit and reviewing drafts. The members are: Amos Doornbos (World Vision International), James Eaton-Lee (Oxfam), Stuart Campo (OCHA HDX), Jenny Caswell (GSMA), Jo Burton (ICRC), Gabriele Erba (UNICEF) and Rosa Akbari (Mercy Corps).

The views expressed in this publication are the authors' alone and are not necessarily the views of the donors or of CaLP member agencies.

CaLP is a dynamic global network of over 90 organisations engaged in the critical areas of policy, practice and research in humanitarian cash and voucher assistance (CVA) and financial assistance more broadly.

For more information, please visit CaLP website at www.calpnetwork.org

Follow CaLP on Twitter: @calpnetwork

FOREWORD

While all humanitarian programmes collect large amounts of data, in Cash and Voucher Assistance (CVA) we collect large volumes of data that is often shared with multiple actors. Much of the data we collect is highly sensitive and private, and we collect it from and about very vulnerable people. It's important to design our programmes and manage data in ways that reduce the possibility that this data is used – accidentally or purposefully – in ways that cause harm or that unfairly exclude designated individuals or groups from benefits.

Types of harm that have been associated with data and digital technologies include:

- **Risk of injury**, for example, when data is used to identify, locate and specifically cause physical, emotional or psychological harm to an individual or group.[1]
- **Denial of services or discrimination** based on data, including opportunity losses and economic losses when data is used for decisions about who is eligible for certain services or benefits.[2]
- **Human rights violations**, such as loss of dignity, liberty or privacy when data is used in ways that dehumanizes individuals, when decisions are made by computer algorithms, or when data collection is invasive or collected, processed and shared without permission, or when individuals must give up their data in return for a life-saving service or to access another right.[3]
- **Deliberate targeting and harassment** of the poor through new technologies. As noted in the Special Rapporteur's report on digital technologies and the welfare state, the use of technologies to identify fraud or violations of the conditionalities imposed on beneficiaries when they receive cash or other welfare benefits allows information to be digitally collected and stored for an undefined period of time. This means that massive amounts of information are held and could used against someone indefinitely.[4]
- **Erosion of social or democratic structures**, for example, through manipulation, amplification of power imbalances or misinformation.[5]

Data management and information sharing are critical components of CVA; we work with sensitive data throughout the entire CVA process. So, in the same way that safeguarding, protection and 'do no harm' are core parts of CVA and other humanitarian programming, data responsibility should be incorporated into all that we do as CVA practitioners. While this toolkit is aimed at CVA, much of the guidance can extend to other humanitarian programmes as well.

BOX 1: WHAT IS DATA RESPONSIBILITY?

Data responsibility goes beyond data privacy and data protection to include principles, processes and tools that support the safe, ethical and effective management of data.[6]

[1] See Microsoft's 'Types of Harm' framework for a deeper look.
[2] See Alston, P. (2019) 'Report of the Special Rapporteur on extreme poverty and human rights', which looks at the role of Digital Technologies and the Welfare State. Presented at the Seventy-Fourth Session of the UN General Assembly, on the topic of Promotion and protection of human rights: human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedom.
[3] See the General Data Protection Regulation (GDPR) (2018) which lists data subject rights, including the right to refuse to have one's data processed, the right not to be profiled with data, the right to not have automated decisions be made that affect one's life, as well as the right to contest automated decisions and ask for them to be reviewed by a human.
[4] Alston (2019).
[5] Microsoft 'Types of Harm' framework.
[6] OCHA (2016) 'Think Brief: Building Data Responsibility into Humanitarian Action'.

Key points to consider:

- **Data responsibility is about more than just data.** Like other valuable goods, data has become a commodity. Individual data points are normally converted into valuable information that is used by different actors for all kind of purposes – those that help and those that harm. A whole ecosystem has grown up around data collected and processed through CVA. Data can confer power and economic benefit to individuals, humanitarian agencies, local and national governments, financial service providers (FSPs), third-party monitors (TPM), technology companies and non-state actors, all of whom are handle data in CVA.
- **Data responsibility requires contextualization, creativity, capacity and collaboration.** A variety of actors collect, manage, use and share data in CVA. There are different organizational mandates and motivations, power dynamics and levels of skills and knowledge at play. You'll need to find agile and adaptive ways to mitigate risks and harms associated with data, especially in conflict-affected or fragile contexts. Data responsibility will depend on everyone involved in the programme cycle, from individual enumerators and frontline staff through country management teams, FSPs, partners and donors. At times, protecting data can put humanitarian staff and frontline workers at risk, too.
- **Data responsibility is not a solo activity – it requires well-rounded teams.** You'll need to involve different parts of your organization and multiple types of expertise as you consider how to ensure data protection and to mitigate potential data-related harms in CVA. This will require technical skills such as information security, data systems administration, data analysis and architecture; legal and business administration, compliance and an understanding of finance; gender, inclusion, protection and safeguarding; and soft skills like negotiation and consensus-building.

In this toolkit, we offer a range of ways to work data responsibility into programme planning, design, implementation and MEAL (monitoring, evaluation, accountability and learning) activities. The toolkit offers a 'gold standard' to which organizations should aspire and identifies both legal and ethical implications that we should be mindful of in our treatment of data. We recognize that it will not always be possible to achieve the gold standard. There will always be trade-offs in terms of speed, budget and other factors to consider, and we know that CVA practitioners will be pulled in many directions. In those cases in which our organizational capacity falls far short of legal and ethical standards, however, we might need to halt activities because our data collection could lead to harm or because it could break the law.

Data is the extension of a person. We should treat a person's data with the same respect and care that we would treat the physical person if they were standing in front of us.

WHY ANOTHER TOOLKIT?

In 2016, ELAN produced the Data Starter Kit,[7] one of the earliest toolkits to address the topic of data responsibility in the humanitarian and development sectors. The Data Starter Kit has been a core resource for the CaLP community and more widely by data-responsible practitioners around the world. Given how the world of Cash and Voucher Assistance (CVA) has changed since 2016, CaLP felt it was necessary to update the Data Starter Kit to meet the current times. The sheer volume of CVA has increased from $2.8 billion in 2016 to $5.6 billion in 2019, meaning that CVA now constitutes some 18% of all international humanitarian assistance.[8]

There has also been a growing emphasis on quality, and CVA is going through a shift in roles and partnerships. CVA increasingly requires coordination across multiple partners in order to reach scale and sustainability. Stakeholder coordination occurs between various government ministries, UN agencies, Red Cross Red Crescent Movement (RCRCM), INGOs and local organizations as well as each of their respective data systems. CVA involves many more partners and often requires implementing partners to use large, established systems, many of which propose incorporating digital identity (Digital ID) or biometrics for identification. CVA increasingly relies on digital means, so banks, mobile network operators (MNOs), micro-finance institutions, and a variety of new financial-technology providers are more likely to be involved as well.

[7] ELAN (2016) 'Data Starter Kit'.
[8] Cash Learning Partnership (2020) 'State of the World's Cash 2020'.

BOX 2: WHAT IS THE GENERAL DATA PROTECTION REGULATION?

The European Union's General Data Protection Regulation (GDPR) came into force in May 2018. It is generally considered to be the strongest data privacy regulation in the world. Most EU-based organizations are bound to comply with the GDPR, and many countries in other parts of the world are basing their own national privacy regulations on the GDPR. The UN and ICRC are not bound by the GDPR because they have certain privileges and immunities due to their international organizations standing.

The amount of data being collected, stored, used and shared across CVA partners is consistently growing. At the same time, new and updated data privacy laws such as the European Union's General Data Protection Regulation (GDPR) are being developed and passed in countries around the world, and these put in place new requirements for organizations who manage personal and other forms of sensitive data. Awareness about the importance of safely managing data, and our duty of care, responsibility for safeguarding programme participants, and obligation to do no harm with data is also on the rise.

Against this backdrop, we offer an updated Data Responsibility Toolkit to reflect these broad changes.

BOX 3: WHAT KINDS OF DATA DOES THIS TOOLKIT COVER?

The term 'data' in these Tipsheets (borrowing from OCHA[9] and ICRC[10]) includes both sensitive and non-personal data, including:

1. Data about the people affected by a crisis and their needs (e.g., personal data of CVA recipients);
2. Data about the context in which a crisis is occurring (e.g., information about communities receiving CVA);
3. Data about the response by organizations and people seeking to help (e.g., locations of cash distribution or plans for data gathering exercises).

Personal Data is information relating to an identified or identifiable natural person.

Sensitive Data is data that, if disclosed or accessed without proper authorization, could result in:

- harm (such as sanctions, discrimination and security threats) to a person, including the source of the information or other identifiable persons or groups;
- a negative impact on an organization's capacity to carry out its activities or on public perceptions of that organization.

Data will have varying levels of sensitivity depending on context, so we have not offered a definitive list of Sensitive Data points in this guide.

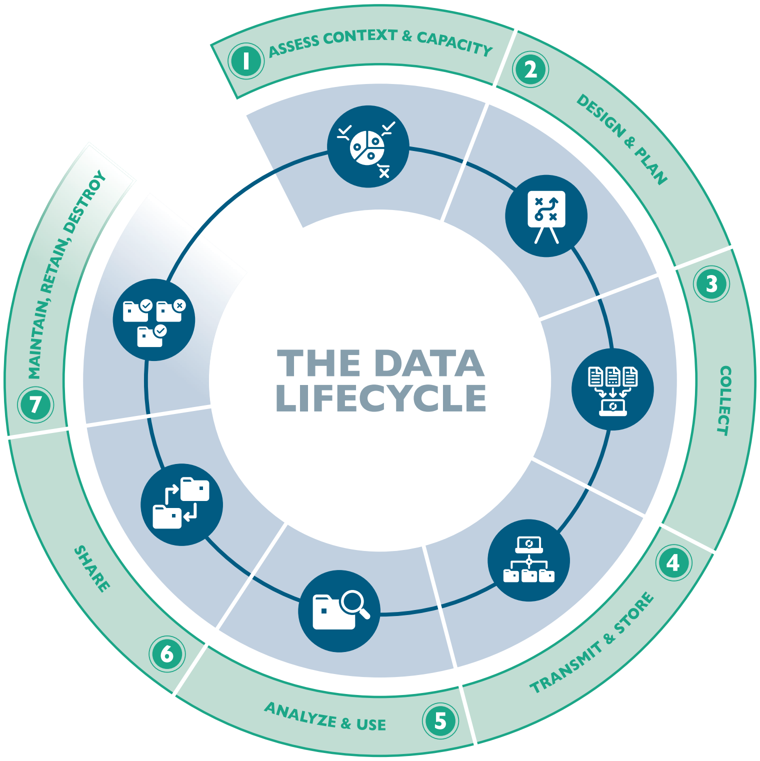
[9] OCHA (2019) 'Data Responsibility Guidelines: Working Draft'.
[10] ICRC (2020) 'Data Protection Handbook'.

HOW IS THIS TOOLKIT STRUCTURED?

In this toolkit, we look at Responsible Data in CVA through the lens of the data lifecycle. It should be noted that the data lifecycle is not a single loop. Rather, it is a visual graphic that helps to guide holistic thinking about data. We expect you will revisit the data lifecycle as your programme develops and you implement additional data activities.

BOX 4: THE DATA LIFECYCLE

The data lifecycle is useful to guide overall data activities for a whole response and for individual data collection activities within different phases of a response. (The lifecycle used here is illustrative. Organizations may have their own version of the data lifecycle.)



For ease of use, this toolkit is divided into 7 tipsheets which address issues of Context and Organizational Capacity; Design and Plan; and Implementation. In brief, the tipsheets cover:

CONTEXT AND ORGANIZATIONAL CAPACITY (TIPSHEET 1)

Early on, high-level decisions need to be made about whether organizations have the capacity to safely and ethically implement CVA. This includes an assessment of the overall data landscape, country context, legal context and power dynamics associated with data in CVA. It also includes an assessment of the compliance aspects, data relationships and systems that will be used (and often required) by donors, consortia, UN agencies, Red Cross Red Crescent Movement (RCRCM), international and national non-governmental organizations (NGOs), governments, financial service providers and other partners in CVA programmes. Organizational capacity assessment at this stage includes the skills, knowledge and resources to protect data and to use digital tools and processes responsibly in the above context. Many of the aspects that we lay out in Tipsheet 1 can be incorporated into existing CVA preparedness and situation analysis studies.

BOX 5: LEGAL vs ETHICAL

When doing something legally, you'll ask *can* we do this? When doing something ethically, you'll ask *should* we do this? Sometimes that which is legal is not ethical.

DESIGN AND PLAN (TIPSHEET 2)

The design and planning phase helps organizations lay out their approach to responsible data collection and management within the various phases of the CVA programme cycle (targeting, enrolment and registration, delivery, and MEAL). Each stage of the CVA programme cycle will likely require some kind of data collection, capture and management along the data lifecycle. For example, needs and vulnerability assessments are usually conducted early on to help agencies to understand the specific needs of the affected populations. These assessments should guide subsequent decisions about the most appropriate cash modalities for the context, the amount and frequency of transfers, partnerships and third party involvement, and the overall process from beginning to end, including which data will be collected and how, and which systems will be used for data storage and analysis. Aspects covered in this phase are aligned with typical CVA response analysis and programme design phases.

DATA MANAGEMENT DURING IMPLEMENTATION (TIPSHEETS 3–7)

Following the design and planning stages, the response moves to implementation. During CVA implementation phases, organizations collect data from affected populations for targeting, enrolment and registration, and delivery of cash or vouchers.[11] They also conduct monitoring activities and gather feedback from affected populations to improve accountability and adapt programming efforts. Data collection during the implementation phase becomes more frequent and more granular. Risks and harms may be exacerbated because of the increased amounts of personal and other forms of sensitive data or group data being managed and shared. Agencies also need to consider what happens to the affected populations' data when a programme closes or is handed over to be managed by another entity, such as when humanitarian CVA programming is transferred to government social protection agencies or other development partners.

Using a data lifecycle approach to guide overall programme data collection and management, and to plan and implement specific data collection and management processes at the different stages of CVA implementation, can help organizations to maximize the benefits of data and to identify and mitigate risks and harms during implementation. Organizations can use Tipsheets 3–7 to develop plans for each stage of the lifecycle, and then return to finalize their overall data design and plan (Tipsheet 2).

[11] Cash programming tends to involve greater amounts of data collection, data processing, and interagency coordination and data sharing, whereas voucher assistance may involve less data sharing because it is often managed in-house and requires less data sharing and coordination with other CVA actors.

LIST OF ACRONYMS

AAP	Accountability to Affected Populations
AML	Anti Money Laundering
CaLP	Cash Learning Partnership
CDR	Call Detail Record
CTM	Counter-Terrorism Measures
CVA	Cash and Voucher Assistance
CWG	Cash Working Group
DPIA	Data Privacy Impact Assessment
DPO	Data Protection Officer
FATF	Financial Action Task Force
FSP	Financial Service Provider
GDPR	General Data Protection Regulation
ICRC	International Committee of the Red Cross
ID	Identification
INGO	International Non-Government Organization
KYC	Know Your Customer
LI	Legitimate Interest
MEAL	Monitoring, Evaluation, Accountability and Learning
MNO	Mobile Network Operator
NGO	Non-Government Organization
OCHA	Organization for the Coordination of Humanitarian Affairs
PEA	Political Economy Analyses
PI	Public Interest
PIA	Privacy Impact Assessment
RCRCM	Red Cross Red Crescent Movement
RBA	Risk Benefits Assessment
SCOPE	The World Food Programme's beneficiary registration system
SOP	Standard Operating Procedures
WFP	World Food Programme
UN	United Nations
UNHCR	United Nations High Commission on Refugees
UNICEF	United Nations Children's Fund

TIP SHEET 1

ASSESS CONTEXT AND CAPACITY

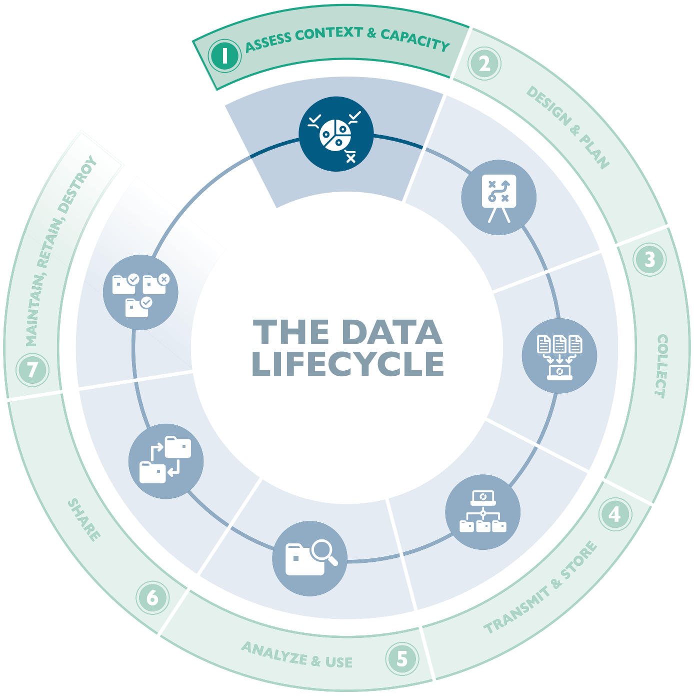
When planning a programme, including one involving CVA, you'll need to assess the overall context you are working in and the capacity of your organization before you go deeper into a detailed programme plan. At this high level, you're interested in determining whether your organization can safely and ethically run a programme in a particular context.

This high-level assessment should include a review of your obligations and capacities to responsibly collect and manage the data that will be needed for the programme. It will likely also include regulatory assessments, feasibility assessments, liquidity and financial service scoping, a look at donor strategies and other topline considerations.

Reviewing context and capacities related to data at this point helps to ensure that you can collect, process and responsibly manage the data you will need to implement the programme and to understand what the trade-offs might be so that you can make key decisions. A high-level assessment of the areas laid out below can help determine if you are responsibly equipped to move forward with a proposal or response. If on first examination, the data-related risks and harms (to affected populations, your organization, partners or staff) outweigh the benefits, you should re-design, re-negotiate or re-think the programme before proceeding to the proposal stage. The key areas below might already be included in your customary pre-proposal research and decision-making processes, but we list them anyway as organisations often do not focus sufficiently on data responsibility as part of their pre-proposal processes.

IDENTIFY THE HIGH-LEVEL PRINCIPLES THAT GUIDE YOUR ORGANIZATION'S APPROACH

Humanitarian actors have already developed or adopted different sets of principles that can help you with high-level thinking about data responsibility in CVA programming. Your organization may follow one or more of these, or it may follow its own principles. High-level principles can help you to later define the operational-level 'red lines' that your organization refuses to cross and aspects that come into play in your 'go – no go' decisions.



Tipsheet 1 offers guidance on how to assess context and capacity related to data before embarking on a CVA programme. Your organization's resources and capacity will determine how in-depth and rigorous your approach to these assessments will be. Even if your resources are limited, it is important to at least consider each of these areas in a rapid set of assessments, as your context and capacity assessment might alert you to a situation where moving forward is ill-advised.

- *CaLP's Protecting Beneficiary Privacy Principles and Operational Standards (2013)*
- *Principles for Digital Payments in Humanitarian Response (2015)*
- *UN Personal Data Protection and Privacy Principles (2018)*
- *EU's General Data Protection Regulation (GDPR) Data Protection Principles (2018)*
- *ICRC Data Processing Principles (2020), pages 35–43*

Principles should be embedded into business processes. As you work through this Toolkit, review and establish where your organization's principles and policies fit in to your operations. Are there any translational documents or steps, such as checklists, risk assessment frameworks or triage tools related to data responsibility, that you might need to embed into existing processes? Is there anyone you can go to for advice when you have questions?

Some organizations might consider establishing an internal data ethics committee that reviews programmes for ethical data use and other ethical aspects. Here is some guidance for **setting up an ethics committee** to review responsible data and technology use.

UNDERSTAND THE POLITICAL ECONOMY OF DATA IN YOUR OPERATING CONTEXT

Data is power. In most humanitarian contexts, whoever controls the most data has the most power and takes control of the response. This can mean that agencies compete over data and push to have certain systems adopted to centralize its management. Agencies who hold the most data or promote their systems as the default tend to be in a better position to access funding. Single entities with large data sets are also able to negotiate more readily with local authorities in situations where humanitarian CVA is being integrated with government social protection efforts. In a time of dwindling funds for aid work, data is a source of tension because of the power and funding it can confer.

BOX 6: WHAT IS A 'POLITICAL ECONOMY ANALYSIS' (PEA)?

A Political Economy Analysis (PEA) is a structured way to examine power dynamics and the influence of economic and social forces in a particular context. PEA is a process of understanding contextual dynamics and how different interventions or prospective interventions (including humanitarian ones) might interact with and influence those dynamics. PEA includes reflection on aspects such as:

- foundational influences (such as history or geography);
- the impact of immediate events and actors (such as leadership changes or natural disasters);
- and the institutional framework (encompassing formal laws and informal practices) that shapes the behaviours and outcomes observed.

PEA encourages practitioners to consider these dynamics, incentives and interests and reflect on how they might help inform operational practice. CVA actors might want to cover the country or regional context as well as the power dynamics and economic and social forces at play within a humanitarian response, including CVA.[12]

Governments are also interested in data for various reasons. This includes both beneficial uses of data for better programming and decision-making as well as less positive uses such as manipulation of lists of CVA recipients, competing for power with non-state actors during conflicts, or harmful targeting of individuals or groups. The private sector and FSPs might also want to access data in order to target potential new customers with products and services, conduct research and development for new products, or monetize data by selling it to others.

Understanding the role that data plays in your working context is important for determining potential risks and harms that can result from data collection, processing and sharing. This in turn can help you to highlight areas where you have space to negotiate for greater data responsibility. Conducting a 'Political Economy Analysis (PEA) of Data' in relation to CVA is a way to set out some of the underlying dynamics that affect how data is accessed and controlled. A PEA of Data might be conducted by a third-party monitor or an external consultant or in some cases a private sector partner. Well-functioning Cash Working Groups can serve as a neutral space for discussing the PEA of Data and for agreeing on collective approaches to data that benefit the

[12] Menocal, A. et. al (2018) 'Thinking and Working Politically through Applied Political Economy Analysis: A Guide for Practitioners'. USAID.

affected population rather than approaches that are more weighted towards serving the agendas of particular agencies or governments. Less powerful agencies may want to conduct a PEA of Data on their own and use it to strategize ways to navigate the power dynamics in the CVA space. Alternatively, a PEA of the wider, general context might be conducted; in this case, it should include an analysis of the PEA of Data as one of its analytical lenses.

BOX 7: SAMPLE QUESTIONS FOR CONDUCTING A POLITICAL ECONOMY ANALYSIS OF DATA FOR CVA[13]

- **Roles and responsibilities.** Who are the key stakeholders? What are the formal and/or informal roles and mandates of different players? What is the balance between different actors in controlling data?
- **Ownership structure and financing.** What is the structure of the CVA response? What is the balance among agencies, governments and other actors in terms of access and control of data? How is CVA financed and by whom? What interests do those who are funding or financing CVA have? How is it influenced by other agendas (e.g., austerity, concern about fraud and taxpayer funding, global level alliances and vested interests of certain countries in the development or political situations of other countries)? If one agency owns and finances all CVA, what does that mean for data responsibility?
- **Power dynamics.** To what extent is power vested in the hands of specific individuals, agencies or groups? How do different interest groups (FSPs, UN agencies, RCRCM, INGOs, NGOs, technology and data companies, affected populations, governments, the media, regulators, etc.) seek to influence how data is managed and who accesses and controls data?
- **Historical legacies.** What is the past history of the various actors in this programming context or the country? What are the historical relationships of the various actors? How does this influence current stakeholder perceptions?
- **Corruption and rent seeking.** Is there significant corruption, fraud and rent seeking in the humanitarian sector, CVA programming or in the country overall? What is the role of data in this? Where is this most prevalent (e.g., at point of targeting, enrolment, delivery, procurement)? Who benefits most from this? How is patronage being used?
- **CVA delivery.** Who are the primary beneficiaries of CVA delivery? Are particular social, regional or ethnic groups included and/or excluded? Are subsidies provided, and which groups benefit most from these?
- **Ideologies and values.** What are the dominant ideologies and values that shape views around the humanitarian sector or in CVA? To what extent may these serve to influence how CVA is being delivered?
- **Decision-making.** How are decisions made within the humanitarian sector or in CVA? Who is party to these decision-making processes?
- **Implementation issues.** Once made, are decisions implemented? Where are the key bottlenecks in the system? Is failure to implement due to lack of capacity or other political economy reasons?
- **Potential for reform.** Who are likely to be the 'winners' and 'losers' from particular decisions around access to and control of data? Who is likely to resist the current set up and who would resist change and why? What could be negotiated to overcome this opposition?

Depending on the situation, you might conduct a more formal PEA (for example, by hiring a third party or agreeing with partners to conduct one jointly); or, if your team is experienced in CVA and the context, you might run a PEA workshop, with representation from a diverse group of CVA actors, to pull out and assess major themes.

Ideally, a PEA of data (or learning from it) would be integrated into your CVA situation analysis, CVA appropriateness and feasibility study, and risk-benefits-harms assessment. It should guide your organization's decision-makers on data-related issues to consider before signing a contract or agreement to engage in a response (e.g. a 'go or no go' decision). You will likely need to do some internal advocacy to help decision-makers become more aware of the need to be 'data ready' before engaging in CVA.

DETERMINE WHICH NATIONAL DATA PRIVACY AND OTHER LEGAL FRAMEWORKS APPLY

Increasingly, countries around the world are developing or updating data privacy laws to adapt to new realities of digital societies. CVA actors need to be aware of these and careful to follow them. Reviewing data regulations might be a part of your habitual regulatory assessment. If not, you may wish to review the areas below. While accountability mechanisms for data privacy laws may be weak in some contexts, violating a data privacy law could lead to an organization being fined or banned from operating.

[13] Adapted from Asian Development Bank's Guidance Note on Use of Political Economy Analysis for ADB Operations (2009). See the full publication for more on PEA. Sources: J. Moncrieffe and C. Luttrell. 2005. An Analytical Framework for Understanding the Political Economy of Sectors and Policy Arenas. London: Overseas Development Institute; V. Fritz, K. Kaiser and B. Levy. 2009. Problem-Driven Governance and Political Economy Analysis: Good Practice Framework. Washington, DC: World Bank.

European-based agencies may be bound by the EU's General Data Privacy Regulation (GDPR), which is considered to offer the highest level of data protection in the world. Agencies like the UN and ICRC enjoy certain legal protections aimed at helping them maintain confidentiality and neutrality in their operations.[14] While their immunity means that they are not bound by the GDPR, the UN and ICRC have their own data protection policies which need to be adhered to.

It can be complicated to manage multiple legal jurisdictions in one response. Working with legal teams and mapping where data crosses borders and which populations it relates to can help you to comply with these laws and combinations of laws. Some contexts, for example Bangladesh and the Philippines, have requirements which conflict with the GDPR. Additionally, some regulations require that Data Privacy Impact Assessments (DPIA) be conducted if certain thresholds are reached related to the type and quantity of data collected and processed, level of sensitivity of the data, or if data is collected from vulnerable populations. They might also require assessments that demonstrate that the collection and processing of data does not lead to harm or infringe additional rights, such as privacy rights.

Some national legislation includes regulations related to data transmission. Data transmission might happen within and between offices in country or across countries. In all these cases, there are special rules that exist to protect the privacy and security of personal or sensitive data that is being transferred. When data transfers happen across country borders, this is referred to as a *cross-border data transfer*. Some countries have laws aimed at restricting cross-border data transfers. Kenya, for example, has enacted a *data localization* law that restricts the types of data that can be transferred out of the country. The EU also has specific rules for where and when the data of EU citizens can be transferred out of the EU. Some countries require a copy of data to be stored locally, or for data to be processed in the country, or for government consent to be obtained before data is transferred out. International organizations also have rules about when and how cross-border transmission can happen.

In some situations, organizations may encounter risks associated with keeping data stored in country, for example, if a government is persecuting a particular set of individuals or groups, and the data that has been collected could be used by the authorities to identify or locate those groups, or if the security situation has deteriorated to the point that the organization does not feel it can keep data secure and protected in the country. In these cases, organizations need to make difficult decisions about following laws versus putting people at risk, and they may decide to avoid collecting data in these cases.

BOX 8: KEY ASPECTS TO REVIEW WITH REGARD TO DATA PRIVACY AND SECURITY IN PRIVACY REGULATIONS

- Kinds of data covered in laws and policies
- Restrictions on types of data that can be collected
- Requirements to understand and assess risk and impact to rights of individuals
- Specific rules about children's data or other special category data like biometrics
- Specifications on data sharing
- Responsibilities/liabilities for those who collect versus those who process data
- Restrictions on whether data can be transferred out of the country
- Restrictions on where and how data can be stored or for how long
- Rules related to whether governments must be allowed to access data
- Orientation on how to collect and record consent
- Fines or other punitive measures that can be applied for mishandling data
- Rights of 'data subjects' (those whose data is being collected or processed)
- Mechanisms required for handling complaints
- Indications on when, how and to whom data breaches must be reported
- Requirements to hire or assign a data protection officer

[14] The privileges and immunities that the ICRC and UN agencies enjoy include immunity from legal process. Their premises, documents and data are also protected from being accessed by governments in the territories where they operate. Their staff are exempt from testifying or providing evidence in legal proceedings. See the Convention on the Privileges and Immunities of the UN (1946) for example and read more about the ICRC's legal standing.

In addition to privacy laws, national legislation stemming from the Financial Action Task Force (FATF)[15] or consumer due diligence rules such as Know Your Customer (KYC) requirements might mandate that you collect certain information in order to conduct cash transfers (see Tipsheet 3 for more on FATF and KYC requirements).

Work with your legal, privacy and IT teams to find the options for data transmission and storage. Review where and how third parties you are working with transmit and store data.

ITIF's publication **Cross-Border Data Flows: Where are the Barriers and What Do They Cost?** provides a list (as of 2017) of countries with data localization policies or laws. You can also check DLA Piper's **Data Protection Laws of the World** (consistently updated) or Deloitte's (2017) **Privacy is Paramount: Personal Data Protection in Africa**.

You might need to weigh difficult choices and trade-offs, for example, if you are legally required to share data with governments and you fear this could place affected populations at risk or influence their levels of trust in your organization. See CaLP's **'Data Sharing with Governments'**.

RESEARCH DONOR DATA, SYSTEM AND GRANT COMPLIANCE REQUIREMENTS

Donors increasingly require CVA actors to coordinate and share data. Donors may also have specific requirements on the kinds of data that agencies must collect and share or how they expect data to be protected. These will normally be outlined in grant agreement documents and will influence how your CVA data can be managed and stored. Some government donors, for example, require CVA recipient vetting or compliance with Counter-Terrorism Measures (CTM) or Anti Money Laundering (AML) regulations; requirements which can put individual CVA recipients at risk due to the amount of personal and sensitive data that is collected for running these checks, lack of clarity about who can access these types of databases, and the potential for inclusion or exclusion errors. Others require certain programmatic data to be shared with them in specific formats and time frames, and organizations will need to anonymize or otherwise treat data before sharing so that CVA recipient data is protected. Researching donor data requirements might already be a part of your feasibility assessments; however, sometimes organizations do not look closely enough at requirements that are specifically related to data.

Additionally, for some grants or partnerships, partners are expected to input data into specific UN systems e.g., the World Food Programme's SCOPE,[16] UN Refugee Agency/UNHCR's PRIME/ProGres[17] and/or UNICEF's Primero.[18] In other cases, data sharing will happen bilaterally among NGO actors through consortia mandates, governance structures and data sharing agreements. Often, UN systems are set up for the collection of biometric data. Data sharing and the use of these systems has been an area of tension among UN agencies and some implementing partners who have concerns about the data protection and security robustness of certain data platforms. Some NGOs have expressed frustration about power imbalances and space to negotiate around UN requirements, as well as UN privileges and immunities. The topic of data sharing and use of these data systems is one of constant flux against the backdrop of ongoing conversations and negotiations. Currently WFP, UNHCR and UNICEF are working on ways to make their systems interoperable with one another and with governments, which has raised data responsibility concerns among implementing partners.

It is important at the pre-proposal phase to understand what donor requirements are and whether they align with what your organization is and is not willing to do. By doing your research before proposal development, you can decide whether to proceed and/or how to negotiate donor data requirements.

Many donors have expressed that they are open and willing to change data requirements if legitimate concerns are raised. By doing your research and then framing or documenting any concerns, you will have a stronger case for approaching a donor to negotiate.

You may face pushback from other parts of your organization which have a lower awareness of the risks that data can pose during implementation. It's important to build alliances inside your organization to advocate for greater data protection and responsible data management and to find ways to engage allied teams, such as safeguarding, protection, legal, IT and cybersecurity, to build more support for data responsibility.

[15] See Financial Action Task Force (2020) 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations'.
[16] See the World Food Programme's overview of SCOPE.
[17] See the UN Refugee Agency's Guidance on Registration and Identity Management 3.6 Population Registration and Identity Management Eco-System (PRIMES).
[18] See the UNICEF Primero website.

REVIEW ORGANIZATIONAL DATA MANAGEMENT CAPACITY

Humanitarian responses, including CVA, depend on multiple actors, and data protection is only as secure as the weakest link. Strengthening of data protection policy and practices is becoming increasingly important as organizations and responses become increasingly digitized and collect and share greater volumes of sensitive data.

Organizations will have varying levels of data management capacity. This does not depend on the size of the organization, but rather on the importance that it has attributed to this area and its access to institutional funding over time for improving data infrastructure and systems. **It is critical that organizations do not collect data that they cannot keep safe. This is a core concept of data responsibility.**

An organizational review can help you to determine whether your organization and your potential partners have the capacity to manage data responsibly in the context in which you are working. This should be done before there is a formal engagement or commitment to deliver CVA in a given context.

You can conduct a thorough assessment of your (or your partner organizations') data maturity using the **Responsible Data Maturity Model for Development and Humanitarian Organizations model** developed for CARE. A broad organizational review and strengthening plan requires time and long-term investment.

If your organization is not able to conduct a full or separate assessment, you could include a section on data responsibility capacity in your general CVA feasibility assessment. The template in Box 9 below can help identify the core questions to include.

This **printable checklist from the Electronic Frontier Foundation** can help you to assess a data processing partner's data security and privacy capacity. It might also help you to assess a third party or an FSP.

This **set of questions** serve as a guide for inquiring about a third party or vendor's GDPR compliance.

DECIDE ON 'GO OR NO GO'

Based on the above research and assessments, aimed at better understanding your context and capacities, determine at a high level whether or not to proceed to the proposal or partnership stage and whether to engage in a particular response.

As noted, if your organization already conducts feasibility, capacity or risk assessments, the above aspects can be integrated into those. It is important that data responsibility is specifically assessed so that you are sure it is considered in the decision-making process. This might be a new area of consideration for your organization and might require advocacy with decision-makers in order for it to be discussed at the pre-proposal stage. **It's important to note that some projects might need to actually halt after this initial analysis stage or find modalities that do not collect sensitive data because the capacity to collect it safely does not exist in the organization or the response.**

If your organization does not already have a template or process for determining whether or not to go forward based on the data context and capacity you could use the template in Box 9 below. When filling in the template, rank where you are currently and make recommendations for mitigation actions that could change a 'no-go' to a 'go' decision. If you do have an existing process, the questions below can be incorporated into it so that you are sure that you are covering responsible data in your early assessments.

BOX 9: QUICK ASSESSMENT FOR GO OR NO GO

If your organization does not already have processes, or you need a quick assessment template, this 'go – no go' tool might help. Use it to rate how confident you are that your organization can manage data responsibly in the context of this response. Then, in the boxes, provide comments about why you are or are not confident, and suggest any strategies that would need to be taken to improve confidence, for example, assessing skills, capacity and resources. Use the responses as part of your 'go – no go' decisions or share them with those who are negotiating involvement in the grant. You should try to obtain input from a diverse group, including legal, safeguarding, protection, IT and cybersecurity, data or MEAL, and frontline staff. Your Data Protection Officer and Ethics Committee (or other similar function) should review this template and support with the decision-making. This template could also be used to assess your levels of confidence in your partners.

CONFIDENCE LEVELS (skills, capacity, resources)	LOW	MEDIUM	HIGH
We know how data will be used and we have identified all parties who will have access to data			
We have assessed the feasibility of working in this context without putting CVA recipients, our organization or staff into unacceptable levels of risk of harm from data			
We can comply with national and global legal frameworks			
We can keep data safe while following national and global legal frameworks			
We can comply with donor data protection requirements			
We can keep data safe while providing donors the data that they require			
We can keep data safe in the systems that donors or partners require us to use			
We have the capacity to manage the systems that we are required to use			
We have the overall capacity to manage data responsibly in this context			
Our partners have the capacity to manage data responsibly in this context			

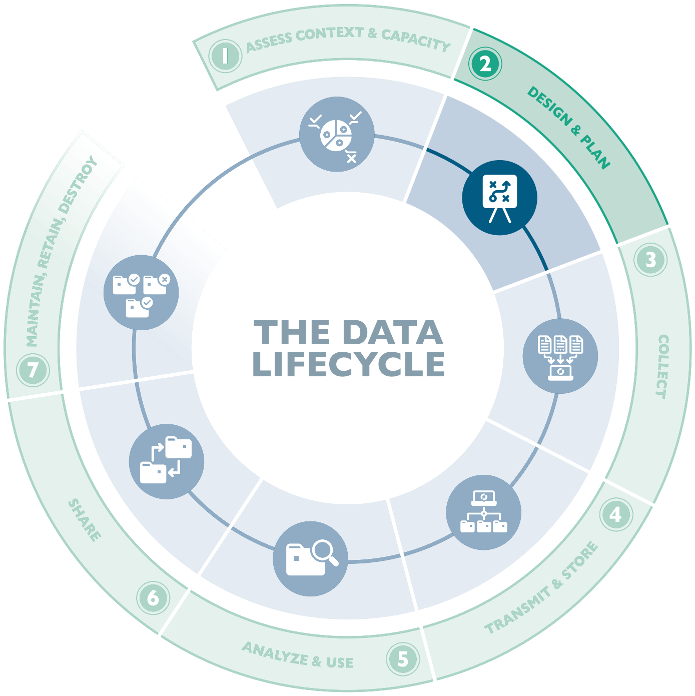
TIP SHEET 2

DESIGN AND PLAN

Once there is a high-level decision on whether the operating context, organizational capacity and conditions related to data allow for a responsible CVA response (per Tipsheet 1) the data collection and management plan for the overall response needs to be designed. The context and capacity assessments in Tipsheet 1 will feed into this phase, where you will be designing your CVA proposal and laying out how data will be managed throughout the response (Tipsheets 3–7 will help you develop the details of each stage of the data lifecycle). At this phase you might also be carrying out cash feasibility assessments, conducting additional regulatory review, doing a market assessment, an FSP assessment, needs and vulnerability assessments, and making decisions on which CVA modalities are the most appropriate and safe for the context.[19]

You will be identifying the partners and other third parties you'll be working with, the systems you will use, what the overall process will look like, and whether humanitarian CVA might link in with government social protection systems. In all of these efforts, you'll want to assess data responsibility. At the same time, various factors related to data responsibility should feed into decisions about how a programme is designed and implemented and if it is safe to collect certain kinds of data or whether the data-related risk is too high for affected populations, frontline workers and enumerators, or for your organization overall.

During the design and planning phase, you'll lay out each of the data processes that will happen throughout the entire response – from needs assessments, through targeting, registration and enrolment, and delivery to MEAL and feedback from affected populations – and how you will responsibly manage data. Design and planning for responsible data will allow you to understand what your response might look like with a fully mature, responsible data approach, to adapt to the time and funding that you have available, and to flag areas that need improving over time. As capacities, capabilities and practices develop, ideally data responsibility will become a mindset rather than a burden.



Tipsheet 2 covers designing and planning. You'll have done the big picture work in Tipsheet 1, and now you will need to go into more detail on what your response will look like in practice. This will feed into your proposal design, budgeting, partner selection and other planning decisions.

[19] See Mercy Corps 'Cash Minimum Standards Policy' for an overview of the various assessments and standards that Mercy Corps incorporates into each phase of a CVA response.

DETERMINE WHETHER YOU WILL USE EXISTING DATA OR COLLECT NEW DATA

As part of your design and planning process you'll want to determine whether you need to conduct an entirely new data collection process, or if there are existing lists or data sets that can be used for targeting, enrolment or delivery. If these lists are out of date, low quality or if they have been altered in an unauthorized manner or only cover a certain part of the population, they will need to be supplemented with additional data or a new data collection exercise. Duplication of data between new and existing lists can be a problem, in which case you'll need to compare lists and assess the situation. If systems are not interoperable, this can be a challenge. In some responses, one organization or agency might already have compared and complied lists and data, yet it may still be a good idea to advocate that data be updated, reviewed for quality or more inclusive.

If your response is linked with an existing social protection initiative, harmonization of humanitarian data with government data will be required. This raises concerns about government access to humanitarian lists. For example, lists of internally displaced populations (IDPs), refugees and migrants, might bring risk of targeting, detention, deportation or other types of abuse by governments. If you are planning to use existing data, it will be important that you review the legal aspects of accessing and using data collected for one purpose to fulfil another purpose. (See Tipsheet 2, Boxes 12 and 13 on Lawful Bases for Data Processing).

COVID-19 has pushed many agencies to use existing data sets and to innovate across humanitarian CVA and social protection. Some of these innovations are set out at SocialProtection.org and on this **blog post** in particular.

Mercy Corps provides **guidance on different types of data that can be used or reused for remote targeting** along with the **pros and cons** of each source.

See CaLP's **case study on emerging approaches for using non-traditional data for CVA targeting**.

The GovLab documented how they conducted a **'data assembly'** to better understand cases in which residents of New York City would be comfortable with access and reuse of their data during the COVID-19 crisis. This methodology could be used in other contexts as well.

DECIDE WHO WILL ACT AS DATA CONTROLLER(S) AND DATA PROCESSOR(S)

At the outset of a CVA response, it will be critical to understand who will act as data controller and who will act as data processor, or whether there will be joint data controllers. The data controller is the entity that makes decisions about how personal data will be processed. The processor takes instruction from the controller on which personal data is collected and how it will be processed. When organizations act as joint controllers, they decide together the purposes and means of processing the same personal data.

BOX 10: ROLES AND RESPONSIBILITIES OF DATA CONTROLLERS AND DATA PROCESSORS

An organization's obligations with regard to data depend on the role they play in data collection and processing. Under the GDPR, for example, individuals and supervisory authorities can hold accountable both controllers and processors for failing to comply with their responsibilities under the GDPR.

Data Controller: an entity that alone or jointly with others exercises control over the purposes and means of the processing of personal data is a data controller. Controllers hold the highest level of compliance responsibility for data. They must demonstrate compliance with data protection principles and other GDPR requirements. They are also responsible for the compliance of their data processor(s). Supervisory authorities and individuals can take action against a controller regarding a breach of its obligations. Data controllers are those who:

- Decide to collect or process the personal data;
- Decide what the purpose or outcome of the processing was to be;
- Decide what personal data should be collected;
- Decide which individuals to collect personal data about;
- Obtain a commercial gain or other benefit from the processing, except for any payment for services from another controller;

BOX 10: ROLES AND RESPONSIBILITIES OF DATA CONTROLLERS AND DATA PROCESSORS (CONT)

- Process the personal data as a result of a contract between us and the data subject;
- Make decisions about the individuals concerned as part of or as a result of the processing;
- Exercise professional judgement in the processing of the personal data;
- Have a direct relationship with the data subjects;
- Have complete autonomy as to how the personal data is processed;
- Have appointed the processors to process the personal data on their behalf.

Joint Controller: If two or more data controllers together determine the purposes and means of processing the same personal data, they are joint controllers. However, they are not joint controllers if they are processing the same data for different purposes. Joint controllers must arrange between themselves who will take primary responsibility for compliance with GDPR obligations, and in particular transparency obligations and individuals' rights. All joint controllers remain responsible for compliance with the controller obligations under the GDPR. Both supervisory authorities and individuals may take action against any controller regarding a breach of those obligations. Organizations are joint controllers, in cases where they:

- Have a common objective with others regarding the processing;
- Are processing the personal data for the same purpose as another controller;
- Are using the same set of personal data (e.g. one database) for this processing as another controller;
- Have designed this process with another controller;
- Have common information management rules with another controller.

Data Processor: an entity that processes personal data on behalf of, or under the instruction of, a data controller is a data processor. Data processors do not have any purpose of their own for processing data. Processors do not have the same obligations as controllers under the GDPR and do not have to pay a data protection fee. However, processors do have direct obligations of their own under the GDPR. Both supervisory authorities and individuals may take action against a processor regarding a breach of those obligations. Data processors are those who:

- Follow instructions from someone else regarding the processing of personal data;
- Are given the personal data by a customer or similar third party or told what data to collect;
- Do not make the decision to collect personal data from individuals;
- Do not decide what personal data should be collected from individuals;
- Do not decide the lawful basis for the use of that data;
- Do not decide what purpose(s) the data will be used for;
- Do not decide whether to disclose the data, or to whom;
- Do not decide how long to retain the data;
- Make some decisions on how data is processed but implement these decisions under a contract with someone else;
- Are not interested in the end result of the processing.

(Definitions and checklists are drawn from the Information Commissioner's Office of the UK and minimally adapted)[20]

Determining roles (controller and processor) will be important for subsequent aspects such as data sharing agreements and information transfer protocols. It's also important that, as the response rolls out, it is clear who is responsible and accountable for which aspects of data processing. You'll also need this information to inform individuals and communities about how you'll handle their data.

See this detailed explanation of the responsibilities of data controllers and data processors under the GDPR.

[20] Information Commissioner's Office of the UK (2018) 'Guide to the General Data Protection Regulation: Controllers and Processors'.

BOX 11: COMMON DATA CONTROLLER–DATA PROCESSING SCENARIOS

To determine who is the data controller and who is the data processor, you'll need to answer the question 'Who makes decisions about what systems are used and which data is collected?' Below we illustrate a few possible scenarios for the Controller–Processor relationship.

If a donor or a UN entity and implementing partners are involved, you might see one of these scenarios:

- A hands-off donor/UN agency or funding that is self-supplied – implementing partner as Controller;
- A prescriptive donor or UN entity that asks for specific systems/approaches/data – Donor as Controller, implementing partner (grantee) as Processor.

To some extent, this may be a political decision. Implementing partners who feel they are more principled than their donors/the UN agency may wish to act as controller here, or if they want to reduce liability they may want their donor/the UN agency to act as Controller.

Among NGOs and INGOs:

This may be very simple, or it might be more complicated if the NGO or INGO works in partnership with others – e.g. a consortium related programme. Some scenarios include:

- NGO or INGO works largely on its own with its own field staff and paper/digital 'closed loop' programming. In this case, the pipeline ends here.
- In a very flat consortium where the roles are almost indistinguishable, you might see Joint Data Controllers. However, legal teams may be uncomfortable with this due to the amount of liability it introduces because you can use any of the Joint Data Controller members for the breach of any other. Privacy teams and field teams may find it complex to communicate with one another in this situation, as they inevitably have very different risk appetites
- Where the consortium member has a clear 'lead', they may be controller or lead processor and issue sub-grants to other partners; in this set up the lead carries most risk of liability in the event of a data breach.
- Where the consortium has quite separate roles (e.g., Member A is delivering food security, Member B is delivering legal advice), they may be separate controllers ('Controllers in common'), and simply have data sharing agreements ('for avoidance of doubt')

FSP involvement:

When an FSP is involved there are likely to be two possibilities:

- The FSP has its own obligations (e.g., KYC, or it also sells consumer services to the beneficiaries via open-loop cards) – in which case they may be a separate Controller – in this case, like 'separate roles', this might be with a data sharing agreement for avoidance of doubt/Controller in Common. In this case, it would be ideal to conduct a risk assessment to determine potential liabilities and risk mitigation strategies that could be introduced by involving or endorsing an FSP.
- FSP has few/no other obligations (rare but possible. A service provider like a CVA software/hardware vendor might also fall into this category) – where the FSP may simply be a Processor. It may also be they are a Processor for some activities but Controller for others (e.g., customers may already have debit cards for which the bank is a Controller, but for some activities they act as a Processor for an INGO).

DETERMINE A LAWFUL BASIS FOR DATA PROCESSING *BEFORE* COLLECTING PERSONAL OR SENSITIVE DATA

In order to process personal or sensitive data, you will need to have identified a lawful or legal basis. It can be useful to think of the lawful basis for data collection as a key ethical and legal gateway to the overall data activity – almost a test of social utility which, if failed, suggests that a particular use of data may not be in the best interest of the affected community or individuals. Lawful bases in national laws tend to focus on the balance between the rights of individuals and groups and the 'locus of agency' – in other words, the place where control, power and mandate resides.

In some contexts, lawful basis is very simple and focused entirely on individual choice. Lawful basis in European law and similar contexts, however, is more nuanced and offers different pathways that recognize that sometimes choice is not possible, for example, when there is an overriding public need, a lifesaving requirement or another reason that makes it necessary to collect and process data. When choice is not possible, there are often additional follow-on requirements that need to be met by those who want to collect and process data to ensure that other rights are not infringed.

For these reasons, the right choice of lawful basis is not only an important legal safeguard, but a foundational principle for recognizing and understanding where power lies and defining the root of your activity in social purpose.

BOX 12: LAWFUL BASES FOR DATA PROCESSING

The GDPR, for example, lists six lawful bases for data processing, as follows:

- **Vital interests:** the processing is necessary to protect someone's life in an emergency.
- **Public task/public interest:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- **Individual consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
- **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.
- **Performance of a contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).

The ICRC uses these same basic lawful bases for collecting personal data but combines contractual and legal into one category. The lawful basis must be determined before data is collected, and the lawful basis and purpose for data collection cannot be switched partway through the data collection and processing activities. If this happens, the data that has already been collected will need to be recollected and treated according to the updated lawful basis.[21]

There has been extensive debate in the humanitarian sector about lawful bases, especially regarding when and whether to use consent versus other lawful bases. Generally, the debate centres on the real challenges of securing consent that is truly informed, voluntary and revocable in humanitarian settings due to the power dynamics in humanitarian situations (including CVA), the lack of choice and the difficulty in explaining how data will be processed and shared, among other aspects. This debate, along with further study of regulations such as the GDPR, has led some organizations to use either Legitimate Interests or Public Task/Public Interest as the lawful basis, combined with a positive ethical informed consent approach. See Box 13 for a more in-depth explanation of lawful bases and guidance on which lawful basis might be most appropriate for CVA. *It should be noted that this guidance does not serve as legal advice – it is intended to offer areas for consideration by your data protection office and your legal team when making a decision about lawful bases.*

[21] These lawful bases are drawn from the EU's General Data Protection Regulation. You'll need to check national legislation to determine what lawful bases are for a particular country. Some international organizations, like the UN and the ICRC, have privileges and immunities and follow their own data protection principles, policies, processes and rules.

BOX 13: CHOOSING A LAWFUL BASIS FOR DATA PROCESSING

Much discussion has taken place about the limitations of informed consent as a lawful basis for data processing in humanitarian situations. An emerging view is that other lawful bases might be more suitable than consent. Here we explore that emerging view in detail.

Under the GDPR, certain lawful bases are not likely to be appropriate for CVA. For example, Vital Interests is unlikely to be a strong choice, even for humanitarian use-cases.[22] Likewise, development or humanitarian activities will generally not be 'required by law', making Legal Obligation an unlikely choice. Because agencies generally do not conclude contracts with the communities they work with, Performance of a Contract (with individuals) is an improbable choice.

This leaves three lawful bases for humanitarian action (including CVA), falling into two major groups:

Group 1 – Consent is the one lawful basis which places agency onto the individual.

Group 2 – Public Task/Public Interest (PI) and Legitimate Interest (LI) – place emphasis on balancing the rights of individuals and the needs of organizations or of society as a whole, as expressed through its laws and customs.

Consent

While using consent as a lawful basis does not remove the need for organizations to be accountable, safe or to consider risk, its use effectively asserts that – in the context in which the consent is obtained – individuals are sufficiently empowered to make informed and voluntary choices. The GDPR outlines that for individuals to be able to provide consent, organizations must be able to offer informed, revocable (reversible) choice in a circumstance in which it can be withheld or refused without negative consequences.

There are various challenges to the use of consent as a lawful basis in humanitarian or development contexts. In particular:

- Given the data-centric nature of much programming, there will likely be consequences if a person does not consent to provide data – for example if assistance will not be provided without enrolment or registration.
- Genuine or free choice are difficult to offer, given the power imbalance present, particularly in a humanitarian context.
- It will be rare that a genuine 'right to be forgotten' or withdrawal of consent can be offered – particularly where there are other requirements such as KYC, Aid Diversion, Audit, Counter-Fraud or MEAL, which may require that personal or sensitive data is retained and thus prevent 'forgetting' about the individual.

Legitimate Interest/Public Task/Public Interest

Where choice cannot be offered, but the activity is still a desirable one to fulfil an agency's mission or to uphold a social good recognized as 'public interest', then either Legitimate Interest (LI) or Public Task/Public Interest (PI) might be the appropriate lawful basis.

LI and PI may not appear to belong together, but both represent an an 'Interest', or imperative, as explained below:

- The Organization (LI) may have an interest in upholding the humanitarian imperative or programmatic objectives enshrined in an organization's charter, founding documents, mission or charitable objectives – e.g. an organization might have a *'legitimate interest to serve charitable objectives by delivering lifesaving work to communities by providing in-kind assistance through Cash and Voucher programming which asks for a recipient's name and status in order to evaluate and deliver that aid';*
- Law & Society (PI): A 'public interest basis' might originate in institutional funding from national donors with explicit mandate in law to deliver lifesaving assistance.

Neither LI or PI justifications for data collection override other obligations in law or good data protection practice. The obligation to inform individuals, to employ 'purpose limitation', to be minimal and safe, remains. In fact, GDPR is clear that, if there is another way to achieve the same result (i.e. if you do not need data), a lawful basis will not be valid.

The final choice of lawful basis will in most instances be a combination of an organization's specific circumstances, the local legal context (particularly if it is a non-GDPR situation and the context is more binary) and interpretation of law. **But we suggest that the imbalance of power, external needs such as KYC, and challenging and shifting contexts, all make Consent a poor fit**

›

[22] Recital 46 clarifies that Vital Interests is likely to apply only in a narrow range of 'lifesaving' cases, where processing 'cannot be manifestly based on another legal basis'. Recital 46 explicitly outlines 'humanitarian purposes' as an example of processing that may serve both public interest and vital interests, including for monitoring epidemics and their spread or in situations of humanitarian emergencies. This clearly suggests that for most non-critical care interventions, vital interests is not likely a good choice for humanitarians.

BOX 13: CHOOSING A LAWFUL BASIS FOR DATA PROCESSING (CONT)

for most if not all instances. An 'Interest' approach (i.e. Public Task/Public Interest or Legitimate Interest), combined with a positive, ethically informed consent approach may offer the best of both worlds, by:

- Maintaining high standards of choice for individuals, based on an appropriate, complete and contextually sensitive picture of how data will be used and for what;
- Placing greater burden on organizations to be, and remain, accountable and reflective about their behaviours, the risks they expose participants to and how those may change over time;
- Reinforcing the need for contextual judgement and understanding – in planning, in contextualizing, in acting and in reacting.

INCORPORATE PRIVACY BY DESIGN

While Tipsheet 1 noted the importance of working within high-level principles for responsible data, the GDPR – and privacy advocates – recommends specifically incorporating *Privacy by Design* principles at the design and planning phase. The premise behind Privacy by Design is that privacy cannot be assured only by adherence to policy and regulatory frameworks. It also needs to be incorporated into the design of data collection processes such that the strength of privacy measures are proportionate with the sensitivity of the data being collected and processed.[23] Privacy should be the default in how data processes are designed, not an option that people have to opt in to. The points in Box 14 are a useful reminder of how to design for privacy.

BOX 14: 7 FOUNDATIONAL PRINCIPLES GUIDE THE PRIVACY BY DESIGN PROCESS

1. **Proactive not reactive: preventative not remedial.** Anticipate risks and prevent privacy-invasive events and harms before they occur and design mitigation strategies from the start.

2. **Privacy as the default setting.** An individual does not have to take any action in order to protect their privacy. Privacy is the built-in default mode for all settings.

3. **Privacy embedded into design.** Privacy is embedded into the design and architecture of both systems and business practices. Privacy is an essential component of the core functionality being delivered.

4. **Full functionality: positive-sum, not zero-sum.** Individuals are not forced to choose between privacy and using an application, tool, platform or service. Giving up privacy is not a requirement for accessing the product.

5. **End-to-end security: full lifecycle protection.** Privacy is enabled through protection of the confidentiality of data throughout the lifecycle of the data. All data is securely collected, used, retained, stored and then securely destroyed at the end of the process, in a timely fashion.

6. **Visibility and transparency: keep it open.** Any business practice or technology should operate according to the stated promises and objectives, subject to independent verification. Data subjects are made fully aware of what personal data is being collected, what is done with it, for what purpose(s) and by whom.

7. **Respect for user privacy: keep it user-centric.** Architects and operators prioritize the interests of the individual by offering measures such as strong privacy defaults, appropriate notice and empowering user-friendly options. Listening to users and responding to their feedback is also important.

See this overview for more information about Privacy by Design.

[23] https://www.ryerson.ca/content/dam/pbdce/seven-foundational-principles/The-7-Foundational-Principles.pdf

CONDUCT DUE DILIGENCE ON PRIVATE SECTOR PARTNERS, INCLUDING FSPS AND OTHER THIRD PARTIES

Because data and digital tools are becoming increasingly integral to the day-to-day work of humanitarian organizations, and because data is ever more complex and requires skills that many organizations do not yet have, partnerships with the private sector are increasingly a part of how organizations manage data. Sometimes these partnerships bring funding or in-kind technical expertise with them. Other times, they enable scale and more sustainable initiatives, making them attractive to the humanitarian sector.

CVA is also increasingly being delivered via third party providers. These entities may have an interest in 'doing good', yet their fundamental motive is profit. They might also have obligations to share data under Counter-Terrorism or Anti Money Laundering laws, which might influence how they treat data. In some cases, the private sector will take data privacy and security very seriously in order to maintain customer trust. In other cases, private sector actors might have an interest in monetizing data or reusing customer data to develop commercial products and services. If you have conducted a Political Economy of Data analysis (see Tipsheet 1), it should have identified some of the power dynamics and possible motivations of private sector partners in CVA. In the 'Data Sharing' stage (Tipsheet 6), we discuss how to set up agreements to protect CVA recipient data and organizational data during CVA programmes.

Many humanitarian organizations have partner due diligence processes in place. Some key data responsibility aspects to include in these processes include ensuring that private sector partners:

- Are able and willing to protect data in the way that humanitarian actors require;
- Have strong and responsible policies and practices that protect and secure data;
- Have responded in an adequate way to past data breaches or data incidents;
- Have past, current and future business lines and business models that align with core humanitarian goals and 'do no harm' principles;
- Do not engage in business activities that are harmful to the vulnerable populations that humanitarian agencies are aiming to support (e.g., use data to identify refugees and migrants in order to detain and deport them, create surveillance technologies that are used by governments to target specific populations for harmful actions, or build data models that are used for excluding vulnerable people or specific groups from benefits and services);
- Are firmly committed to working with CVA programmes and recipients in ways that are not predatory or exploitative.

Some private sector partners, for example, many MNOs, have business models that rely on secure data management, and therefore have extensive expertise in the areas of data privacy and security. In some cases, they can help humanitarian organizations improve in this area.

If you'll be working with the private sector on data or technology initiatives, you can use **this Guidance Note** to help you to frame a partnership that has data responsibility at the centre.

This **printable checklist from the Electronic Frontier Foundation** can help you to assess a partner data security and privacy capacity.

This **set of 7 questions** can help you ask your vendor the right questions about GDPR compliance.

ESTABLISH A DATA GOVERNANCE PROCESS TO HELP MANAGE RESPONSIBILITY AND ACCOUNTABILITY FOR DATA

Depending on the structure of the CVA programme and the involved partners, it is important to document who holds responsibility for data management overall and for each data collection process at the different stages of the CVA programme cycle. This includes:

- Maintaining a data inventory list and keeping track of which partners hold which data, and ensuring that they comply with time frames for data retention and destruction, and comply with data sharing agreements and other language in contracts and agreements related to data maintenance, retention and destruction;
- Keeping track of who can access what data, including managing changes in access levels of staff and partners;
- Ensuring that data is aggregated or de-identified as soon as possible after collection or use (depending on the circumstances);

- Managing and responding to any requests from CVA programme participants for data correction, deletion or removal of their data from the system.

Be sure to specify your needs related to data maintenance and retention in the early stages of your planning to ensure that you have the necessary budget for secure data maintenance, retention and destruction. Your role in the project will determine whether this cost is borne by your organization or a partner.

PREPARE FOR POSSIBLE CRITICAL DATA INCIDENTS OR BREACHES

Critical data incidents include breaches of infrastructure, unauthorized disclosure or alteration of data, and the use of data that has been collected for humanitarian purposes for other purposes without corresponding consent or agreement. They happen when the way that data is managed causes harm to affected populations, organizations, staff or other individuals or groups. Data incidents can involve the theft or confiscation of a laptop containing sensitive data, a CVA recipient list being altered or shared without authorization, or forced provision of survey or household-level data to authorities. Data incidents can even occur without technical infrastructure being compromised. When the collection, use and sharing of data leads to the spread of negative rumours, cultural sensitivities, political dynamics and other factors that have adverse effects on affected populations or humanitarian organizations, this can also be considered a critical data incident.[24]

Based on your overall context and capacity assessment (Tipsheet 1) and past experiences, and the types of actors who might be interested in accessing your data, draw up a list of the kinds of data incidents that might occur during the CVA response and plan how you will mitigate these in your planning and design. You will need to raise this issue with partner organizations or (if you are an implementing organization) with agencies who are managing the data systems. **When vetting partners (e.g., FSPs, MNOs, etc.) who will manage digital data tools and wider data systems, it's important to have in writing their responsibilities and liability (and yours!) for critical data incidents as part of your contractual agreement.** Your information security team should be involved to support with this type of vetting, and your legal team can provide templates or wording that need to be included. You are likely to need to involve your Data Protection Officer (DPO), too.

Lastly, you'll want to determine how you will organize to respond to a reported critical data incident – documenting this in a 'critical data incident protocol' that establishes how data incidents will be reported, investigated and communicated. It will also lay out the process you will go through to determine if and how you would offer compensation or support to anyone who has been harmed by a data breach. Most data privacy legislation requires a data breach to be reported to data protection authorities and to those affected by it within a specific time frame. While it has been uncommon for humanitarian actors to disclose critical data incidents or data breaches to affected populations, people have a right to know if their data has been compromised and the types of harm that could result, and to be compensated for damages they may suffer. This area is linked with accountability to affected populations (AAP) in the CVA space, and so teams working on AAP may be good allies in this work. Safeguarding teams are also excellent allies, considering that critical data incidents involve power dynamics and harm. Organizations have a responsibility to prevent data incidents and a duty of care in cases where they happen.

Your data incident mitigation strategies will need to cover data security and data systems as well as training and incentivizing people to protect data. They will require input from staff, enumerators and others who manage data 'on the ground' and who are familiar with the day-to-day context of a response.

Talk with your safeguarding, protection, cybersecurity, data management, data protection, legal, communications/PR and compliance teams to determine how you'll collectively respond to critical data incidents and whether policies of this kind already exist. You might be able to build on your organization's safeguarding or public relations crisis management experiences and protocols to plan for and manage critical data incidents.

Be sure to include critical data incidents on your risks-benefits-harms or Data Privacy Impact Assessment (see next step in this Tipsheet), along with examples of how you will mitigate potential harms.

[24] OCHA Centre for Humanitarian Data. 'Note #2: Data Incident Management'. Guidance Note Series: Responsible Data in Action. 2019.

AFTER PLANNING OUT THE FULL DATA LIFECYCLE (TIPSHEETS 1−7), CONDUCT A DATA PRIVACY IMPACT ASSESSMENT

A Data Privacy Impact Assessment (DPIA) (also called a Privacy Impact Assessment or PIA, or sometimes referred to as a Risks-Benefits Assessment or RBA) is a systematic analysis of the potential privacy risks to which individuals are exposed because of data collection and use during programme implementation.

The DPIA should be carried out during the planning stage, but you'll need to have worked out plans for the full data lifecycle (Stages 1–7) before you will have the necessary information to conduct it.

A DPIA has an explicit focus on the potential harms *to the people whose data is being collected and processed* – it is not a tool for assessing organizational risk and liability. However, if there is a high risk of harm to the individuals and groups who participate in a programme, an organization will accrue risk and liability. A DPIA allows you to analyse threats and risks related to the impact of data and develop mitigation strategies. DPIAs help humanitarians protect participants' privacy and strengthen public confidence in a programme. The EU's General Data Protection Regulation (GDPR) and some other legal frameworks mandate that a DPIA or PIA be conducted in any case where a high risk is likely to exist to the target population. A DPIA helps organizations determine whether the potential benefits of data collection outweigh the possible harms, and it provides a way to document findings. DPIAs should be conducted regardless of the CVA modality.

If your organization is audited for its data management practices, having a DPIA on file helps you provide documentation on how your organization identified and mitigated data collection and processing risks. Where it can be shown that your organization was thorough in its data management and risk reduction, judgments and fines will likely be smaller. If your organization is seen to be acting negligently, then higher fines could be recommended. If a DPIA is not conducted, it is important also to document the reasons why it was not possible.

Your DPIA should be used as a planning tool, along with (or incorporated into) your organization's other risk assessment processes, in order to identify areas of risk for an organization in terms of how its data management could harm affected populations and its own reputation or legal and financial situation. As far as possible, DPIAs should be participatory activities, so that the views of affected populations are included in identifying and qualifying risks and in proposing mitigation strategies. DPIA screening questions (such as 'Is this population vulnerable?') should be incorporated into other processes such as planning checklists, programme design guides, sign-off frameworks and bid approval processes to help mainstream privacy into the wider organization.

If an organization finds that, during the DPIA process, the right support and resourcing are not available to responsibly manage data, data cannot be responsibly collected and used because of the context, or that affected populations are taking on risk from data use that is not proportionate to the benefits, the response should be halted and a different programmatic approach that is less data-heavy should be implemented.

Some organizations will implement the DPIA review as part of their governance structures and frameworks as well. The important thing is that there be a specific data-focused risk assessment that focuses on the impact of data use on affected populations.[25]

While Tipsheet 1 suggests a rapid assessment to determine whether an organization should engage overall with a response based on context and capacity (see Box 9), the DPIA goes in-depth to assess the proposed data collection and use activities, as specified in a proposal plan or a data collection and use exercise within the proposal (for example, a data collection process for targeting CVA, the use of a certain CVA delivery modality, or a MEAL or survey process).

Examples of DPIA, PIA and RBA frameworks and processes include:

- ICRC **Data Protection Handbook**, Appendix 1, page 299.
- Sonjara's **Benefit Risk Assessment Framework Workshop**.

[25] DPIAs can be done at different stages of the CVA programme cycle. An overall DPIA might be done at programme design phase to help determine whether CVA actors are able to reduce privacy risks to an is acceptable level. Potential risks to affected populations should not outweigh the potential benefits. The same goes for organizations – data collection processes should bring more benefit than risk. DPIAs should also be conducted for specific data collection activities throughout the programme cycle. If a standardized DPIA format is used, DPIAs can be carried out periodically, and in a decentralized manner, at the start of new data collection activities. These can be consolidated and periodically used for learning and improvements over time. The DPIA should be a 'living document' that is periodically reviewed, for example if partners, context or data use change.

- USAID’s **Benefit Risk Assessment tool**, pages 11–13 of the Considerations for Using Data Responsibly document.
- **The Privacy Commissioner of New Zealand’s PIA**.
- CaLP’s **Protecting Beneficiary Privacy**, pages 19-20.
- Microsoft’s **Assessing Harm for Tech Builders** framework.

Some organizations use a Risks-Benefits Assessment (RBA), which can be more useful for the humanitarian context, and as long as it covers data privacy aspects, it can often replace a DPIA. RBAs on data examine critical question of who risks and who benefits from data collection in an effort to ensure that the most vulnerable are not bearing the risks while organizations are reaping the benefits. OCHA’s **Note on Data Impact Assessments** covers the different types of assessments and how to determine which is most appropriate in which settings.

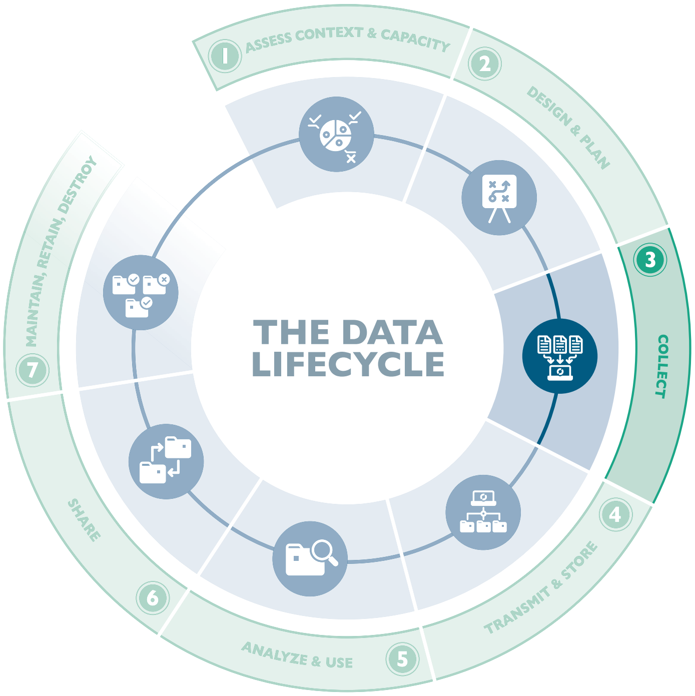
TIP SHEET 3

COLLECT OR ACCESS DATA

Data can be used for good purposes such as improving programme targeting and reducing duplication and fraud. But it can also be used to influence behaviours in non-transparent ways: for extortion, to target both individuals and groups for active harm, and to spread misinformation. Data can also inadvertently lead to harm, despite good intentions. For all these reasons, and because people have a fundamental right to privacy, it is critical to collect and access data responsibly.

Collection of personal and other forms of sensitive data happens at every stage of a CVA programme, including:

- planning and needs assessments
- targeting
- enrolment and registration
- delivery
- feedback
- monitoring and evaluation



Tipsheet 3 covers aspects that will help you collect high-quality data that is necessary and proportionate to the purpose for which it is collected. In cases where you are accessing data that was collected previously or by other organizations, this guidance should still apply.

BOX 15: DATA DEFINITIONS: PERSONAL DATA, SENSITIVE PERSONAL DATA, SENSITIVE NON-PERSONAL DATA AND METADATA

What is personal data?

- Data that relates to an identified or *identifiable* individual; including, data that directly identifies an individual (a name or number or IP address or 'cookie' identifier) or data that could potentially identify an individual (e.g., because the data set is small or because the data includes information or a combination of information that makes it easy to identify an individual within a larger data set)
- Data that identifies an individual when one data set is crossed with another data set.

What is sensitive data?

- Sensitive data includes sensitive personal data, which, if disclosed or accessed without proper authorization, could result in discrimination against or the repression of an individual, the source of the information, or other identifiable persons or groups.

›

BOX 15: DATA DEFINITIONS: PERSONAL DATA, SENSITIVE PERSONAL DATA, SENSITIVE NON-PERSONAL DATA AND METADATA (CONT)

- Sensitive personal data normally includes race, ethnic origin, political affiliation, religion, trade union membership, genetic info, biometrics, health, sex life, sexual orientation; it also includes personal data about highly vulnerable individuals, such as children or displaced people.
- Other personal information can be sensitive depending on context and culture, and in humanitarian contexts much data is highly sensitive. Because data has varying levels of sensitivity depending on context, we do not specify a definitive list of sensitive data points in this Toolkit.
- It's good to consider who decides what is sensitive or not. Affected communities might determine that a particular data field is sensitive even when data privacy regulations or implementing organizations do not label it as sensitive.

What is sensitive non-personal data?

- Data about the context in which a crisis is occurring (e.g., information about communities receiving CVA);
- Data about the response by organizations and people seeking to help (e.g., locations of cash distribution or plans for data gathering exercises.[26]

What is Metadata?

- Metadata is 'data about data'.
- Metadata is produced through the practical arrangements of CVA, and different legal and regulatory obligations apply to the collection, sharing and retention of metadata.
- In the case of mobile money, for example, metadata includes 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 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. It could be used to infer information about affected populations' behaviours, movements, affiliations and other characteristics. The ability to draw inferences about beneficiaries is possible long after a programme ends.[27, 28]

DETERMINE HOW TO PROTECT DATA IF YOU ARE COLLECTING IT REMOTELY OR VIA MOBILE PHONE

While remote data collection has been practised in some countries due to conflict or difficult working environments, this form of collection became more prevalent during the COVID-19 pandemic. Many organizations began conducting CVA targeting via phone calls or relying on community members to identify and manage CVA recipient selection. Confidentiality concerns arise with this type of data collection which can lead to favouritism or manipulation of lists or put community members in a position of having to manage demands for cash. If an effort is fully remote, there will not be an available, external third party (such as a CVA organization) to flag or offer support in these situations.[29] Furthermore, Know Your Customer (KYC) regulations have been waived or reduced in some cases, and when they are implemented, organizations have found these difficult to comply with when registering recipients by phone because they could not directly verify identity. While some of this data is still collected without using remote digital mechanisms, remote collection is a rapidly evolving enterprise, with many of the new efforts involving digital data collection methods. Examples of innovative new practices that are emerging include the use of voice identification or 'selfies' to prove identify. The FATF recently noted that remote ID verification can be equally effective where high levels of ID assurance can be achieved. not an option that people have to opt in to. The points in Box 14 are a useful reminder of how to design for privacy.[30]

[26] OCHA (2019) 'Data Responsibility Guidelines: Working Draft'.
[27] ICRC Data Protection Handbook (2020).
[28] ICRC and Privacy International (2018) 'The Humanitarian Metadata Problem: Doing No Harm in the Digital Era'.
[29] Save the Children Tip-sheet: Adaptations in how we identify, register, and verify CVA beneficiaries in the time of Covid-19. (unpublished)
[30] Financial Action Task Force (FATF) (2020) 'Digital Identity'.

See CaLP's **CVA in COVID-19 contexts** for an overview of how different agencies are adapting to remote data collection and other remote activities.

See **this discussion** of pros and cons and good practices for remote monitoring.

See **this checklist** for guidance on how to safely and security collect mobile data. It can be adapted for mobile data collection for CVA.

The WFP's **Vulnerability Analysis & Mapping (VAM) toolkit** offers guidance on Conducting Mobile Surveys Responsibly.

USE INCLUSIVE DATA COLLECTION METHODS, APPROACHES AND TOOLS

When designing data collection, especially if using digital tools, purposefully designing for inclusion is critical in order to avoid leaving out the most vulnerable populations. Women are less likely to have access to mobile phones compared to men, and this is particularly true in humanitarian contexts. The 2020 Mobile Gender Gap report from the GSMA, for example, showed that women are 8% less likely than men to own mobile phones, and this gap increases to 20% when it comes to mobile internet.[31] These gaps can be even greater in humanitarian contexts.[32] The poorest are likely also be excluded from mobile access. Equally, it is important for organizations to consider whether they are being inclusive of those with disability and other groups who experience discrimination. You'll need to build these so-called 'edge' cases into your data collection process design from the start – and budget for them. This will mean taking steps to design for different kinds of access and actively seeking out 'edge' cases to ensure that you are testing data collection methods and approaches with those groups that are more likely to be left out.

This **IASC Accountability and Inclusion Portal** has resources and guides for ensuring inclusion in humanitarian processes.

See **this toolkit** on ensuring that people with disabilities are digitally included.

The **Gender and Information Communication Technology (ICT) Toolkit** from USAID offers a number of modules and considerations for understanding women's access to ICTs.

You'll need to offer more than one option or pathway for data collection to ensure that the most vulnerable (for example, those who are not easily reached, women, those who don't speak more common languages) and those with disabilities are not excluded.

CONSIDER THE IMPACT OF KNOW YOUR CUSTOMER, SIM REGISTRATION AND COUNTER-TERRORISM MEASURES

When humanitarian organizations collaborate with MNOs and other FSPs, they are required to comply with Know Your Customer (KYC), Anti Money Laundering (AML), Counter-Terrorism Measures (CTM), and other regulations and legislation designed to prevent money laundering and corruption. This means that your organization or CVA recipients themselves must share personal and sensitive data with third parties, including regulators, in order to verify CVA recipient identity. Certain donors require additional vetting as part of CTM. Additionally, over 155 governments around the world have mandatory SIM registration policies in place which require people to provide proof of identity before they can access a SIM card.[33]

The Financial Action Task Force (FATF), the global money laundering and terrorist financing watchdog, may also make additional recommendations, in which case, these are transposed into national law, and new CVA recipients have to be screened against these lists. KYC information must be cross-checked against lists established by local authorities, including individuals and entities potentially involved in a conflict or situation of violence. CVA beneficiaries might be excluded from assistance if a match is found, even if the match is a case of mistaken identity. In conflict settings, families in need of CVA might be from communities that are on these types of watchlists, as they are often classified by geographic zone.

This process may be monitored by public authorities and include reporting obligations. AML and CTM are often enacted with the aid of third party software, yet it is sometimes unclear what happens to the data that is input into these databases. Data collected could be used for other purposes by governments or by FSPs or MNOs, such as advertising of additional financial services (or other services if data is sold or shared onward), or credit worthiness determinations.

[31] GSMA (2020) 'The Mobile Gender Gap 2020'.
[32] GSMA (2020) 'Bridging the mobile gender gap for refugees'.
[33] GSMA (2020) 'GSMA Digital Identity Programme: Insights and Achievements (2016–2020)'.

It is critical that, when negotiating a scope of work and procurement process with an FSP, these important elements are assessed, and that organizations have clear processes in place for reviewing any scope of work documents. This process should be coordinated between the teams which are managing CVA processes directly, technology teams which can assess aspects like security, data storage and server elements, data and privacy leads, and procurement. This can help organizations avoid gaps and loopholes, or surprises; for example, data sharing clauses that do not fully protect CVA data.

Not all donors or country governments require this type of screening, but in cases where this is required, you should explain this to affected people as part of the data collection process and they should be given a choice of whether they want to provide their data or to enrol using a different type of process or to receive assistance in another form, such as in-kind, cash in hand, one-time vouchers, or anonymized smart cards. Not all agencies are able to make this choice, however, as it depends on their structure, size and dependencies on other agencies for systems and funding.

It is possible to negotiate with donors concerning the operational implications of their requirements for screening. Donors are increasingly aware of the need to manage data responsibly and to mitigate risks related to data. They often understand the trade-offs involved, for example, that screening undermines humanitarian principles of impartiality, meaning you will have room to negotiate.

A list of countries that require SIM Registration as of 2020 can be found **here**.

KYC and some examples of adjusted regulations are discussed in this **Tipsheet** from 2016.

TAKE EXTRA CARE TO CONSIDER COSTS AND BENEFITS OF COLLECTING BIOMETRICS OR INTRODUCING DIGITAL ID SYSTEMS

A number of benefits are cited when biometrics are used for managing and tracing enrolment and delivery of humanitarian aid, including CVA. Biometrics, such as fingerprints, iris scans, facial recognition and voice biometrics, are all being used as part of CVA programming in different parts of the world. They offer one form of unique identification for an individual, even if there is no other means to prove their identity because their other identification documents have been lost or are otherwise unavailable (often the case of displaced people). While biometrics have been promoted as a way of reducing individual fraud, critics note that they do not tackle corruption and wider abuse at a systemic level, where it is suspected that most fraud happens.[34] Additionally, biometrics have been questioned for offering efficiencies for agencies without delivering incremental benefits to affected populations[35] and for a number of other reasons such as inaccuracies, risk of function creep and the possibility that biometric data could be shared with governments. Some organizations are exploring the use of privacy-preserving technologies, cryptology and distributed ledger systems (DLTs) such as blockchain as a way to more securely hold biometric data, but more work is needed in this area.

If using biometric data, it must be proportionate to the purpose for which is it being collected, and organizations should be able to prove that the benefit in using biometrics outweighs the risks of their use. Because of the highly sensitive nature of biometrics, you will always need to conduct a DPIA, PIA or RBA before confirming the use of biometrics. If, as an implementing agency, you are required to use biometrics because the system that you are feeding data into requires it, you will need to carefully review your capacity to securely collect and manage biometrics, and agencies asking their partners to use biometrics must ensure that those partners have the capacity to protect biometric data. Because there is a level of discomfort with biometrics among some affected communities, it is of critical importance that individuals are given a free and meaningful choice about whether they will provide biometrics in return for enrolling in or receiving CVA, and that you also provide an alternative that does not place a burden on the individual. Other forms of identification that serve the purpose of unique identity but do not involve biometrics are being explored by organizations such as Mercy Corps. If exploring the use of biometrics, be sure that you fully understand how a given solution works, from end to end. If the solution is too difficult to understand, that may be sufficient reason to fall back to non-biometric forms of ID. The ICRC has conducted an in-depth exploration of when and where it might be appropriate to use biometrics and identified some instances in which they are appropriate, and some in which they are not.

[34] Oxfam and The Engine Room (2018) 'Biometrics in the Humanitarian Sector'.
[35] See Access Now's Open Letter on 'Why ID' for more on the challenges of biometrics in humanitarian work and other situations.

Mercy Corps **Internal Primer on Biometrics** offers detailed guidance.

See Chapter 8 on Biometrics in the **ICRC's Data Protection Handbook** for a thorough discussion of biometrics and how to handle this type of sensitive data and under what Lawful Basis biometrics can be captured in different circumstances.

See **this paper** for a thorough discussion of the use of biometrics and identification and registration systems in protracted and recurrent crises.

Read this **'Open letter to to the leaders of international development banks, the United Nations, international aid organisations, funding agencies, and national governments'** for a more in-depth review of some of the core questions and issues with biometric ID systems.

COMMUNICATE TRANSPARENTLY WITH AFFECTED POPULATIONS ABOUT DATA COLLECTION AND PROCESSING

Transparent and clear communication with affected populations about data collection and processing is an important part of any data process and should be integral to how you design and budget for responsible data management. As noted in Tipsheet 2 in the section on lawful bases (see Boxes 12 and 13, pages 20 and 21), the use of consent as a lawful basis for data collection and processing is being contested. However, regardless of which lawful basis you use for data collection and processing, you will need to be able to transparently explain to affected communities (in culturally appropriate ways) who is mandating the data collection, how to contact them, why the data is being collected and processed, whom to contact in case of any questions about data processing, and with whom the data will be shared, especially if it will be shared with authorities, government bodies such as law enforcement, or entities in another territory or jurisdiction.

BOX 16: WHAT SHOULD AFFECTED PEOPLE KNOW BEFORE THEY PROVIDE THEIR DATA?

The ICRC policy mandates that the following information be provided to affected individuals when Consent is the legal basis:

- the identity and contact details of the organization that has mandated and controls the data collection and processing (the 'data controller');
- the specific purpose for personal data processing;
- an explanation of the potential risks and benefits of the data processing;
- that the data controller may process personal data for other, similar purposes (indicate what those purposes might be);
- that consent can be withdrawn at any time;
- circumstances in which it might not be possible to treat personal data confidentially;
- rights to object to the processing of their data; rights to access, correct and delete personal data;
- how to exercise their data-related rights and possible limitations on the exercise of those rights;
- to which third countries or international organizations their data might be transferred in order to achieve the purpose of the initial collection and additional processing;
- how long the personal data will be kept (or the criteria that will be used to determine how long it will be kept) and any steps taken to ensure that records are accurate and kept up to date;
- with which other organizations, such as authorities in the country of data collection, their data may be shared;
- an indication of the security measures implemented by the data controller regarding the data processing.[36]

You'll need to simplify any communication about how data will be processed and stored into clear and accessible language that is meaningful for affected individuals and communities. Drawings, videos and audio consent processes might help. You will want to be aware that individual consent and privacy are concepts that translate differently according to culture. Some

[36] ICRC Data Protection Handbook (2020).

staff working on CVA have criticized European, legal approaches to consent and privacy for being Northern and perceived as patronizing, and often not useful or valued as a result. The single most important thing when aiming for transparency about data collection and processing is to ensure that the affected population fully understands the process, rather than simply conducting a checklist exercise.

Be sure you include information about data collection, data rights and complaints mechanisms in your overall feedback and accountability processes for any CVA programme. This includes information about the metadata (see definition on page 26) that will be collected through digital CVA programming or data collection.

This toolkit can help you to design a responsible data communication and outreach plan for your response.

If you are offering a complaints mechanism – and you should be! – be sure that you have planned for staff, systems capacity and budget for implementing it. For example, if someone wants their data removed from your system, are you able to find them in your system, verify their identity and comply with their request?

For more on consent, see World Vision's **Informed consent sheet**.

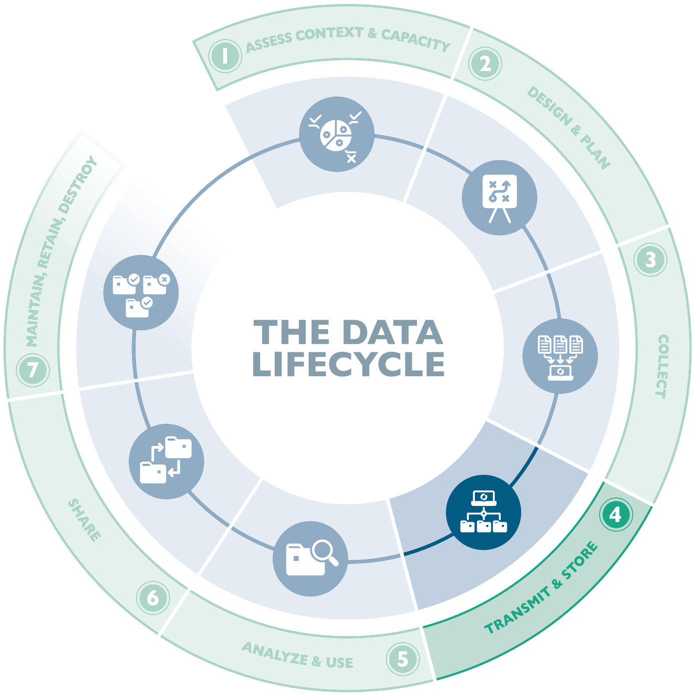
See the ICRC's **Data Protection Handbook** for more ideas on how to manage informed consent and other lawful bases, along with templates and language to adapt to your situation. Chapter 9 of the Handbook provides detailed orientation on CVA and data protection as well.

Find out more about **Inter-Agency Community-Based Complaints Mechanisms**.

TIP SHEET 4

DATA TRANSMISSION AND STORAGE

Data transmission happens whenever data is passed between one place and another, for example, when employees of your organization pass data or files to each other, to another organization, or to a government or other entity. Sometimes data transmission is an active process, for example, when an enumerator presses 'send', so that survey data moves via the mobile network from a mobile phone to an organization's server or to the cloud. Other times it happens behind the scenes because a mobile device, application, website or back-end software transmits data automatically while someone is using it, for example, when location data is transmitted to a mobile network operator because a mobile phone pings a nearby cellphone tower. Storage of data normally happens on a device (such as a mobile phone, laptop), on a server, or in the cloud.



Data collected during the various steps of a CVA response (needs assessment, targeting, enrolment and registration, delivery, feedback and MEAL) will be transmitted and stored in different ways, depending on how your data collection process is designed. Data can be at risk during both transmission and storage for various reasons, so it's important that you transmit and store data in secure ways that limit who can access it. CVA practitioners often work with partners and third-party applications, and you'll need to ensure that the data collected from affected populations is not vulnerable to unauthorized access, alteration, deletion or sharing in ways that create potential for harm. Data transfer agreements can help to formalize the transfer of data between CVA actors.

In Tipsheet 4 we explore how to minimize the risks associated with data transmission and storage.

FOLLOW BASIC DATA SECURITY RECOMMENDATIONS FOR DATA TRANSMISSION AND STORAGE

A number of basic data security protocols should be used by anyone who is collecting, transmitting or storing data. CVA practitioners should look first and foremost to their institutional policies and guidance on data security and ensure compliance with these in addition to other legal, regulatory and best practice standards.

BOX 17: WAYS TO PROTECT DATA WHEN USING DIGITAL TOOLS AND APPLICATIONS

- Avoid building new tools and bespoke applications, as these may require intensive resources to ensure security, manage and maintain security, and test for possible flaws.
- Don't use a system or tool simply because a partner, peer organization or funder requests it – work with your IT security team and privacy officer first to ensure that it is secure.
- Plan sufficient time and resources to conduct security assessments on tools and platforms.
- Only use secure, private Wi-Fi networks or connect via a virtual private network (VPN).
- Encrypt devices and transmission of data, use encrypted messaging apps such as Signal.
- Use two-factor authentication.
- Only visit secure websites (those that use https – not just http – in their address).
- Use strong passwords, and don't share passwords or use a single login and password for multiple people.
- Use vetted organizational systems for encrypted data transfer and storage (for example, Microsoft SharePoint for file transfer instead of third-party file-sharing programmes).
- Use privacy-first browsers and search engines (Firefox and DuckDuckGo).
- Keep your software and virus protection up to date.

Your IT security team will be able to guide you on the most secure ways to transmit and store data. You may need to work with your IT teams at headquarter level to identify some of the contextual challenges so that informed trade-offs can be made in the case that data security clashes with ease of operations, making it more likely that people will bypass security to facilitate working practices. This is a key area to outline in your DPIA or RBA (see Tipsheet 2). Data security might not be top of mind for staff and enumerators, especially in situations of high stress and conflict. Higher technical security measures tend to slow down systems and processes, and staff might be compelled to find ways around them to speed up their work. It's critical that your organization emphasizes the importance of following mandated security measures, and opens dialogue with staff and enumerators to design security measures that are likely to be followed and do not unnecessarily burden their workload.

In conflict situations, even the best security measures might be unsuccessful because enumerators or staff are physically threatened by those who want to access CVA recipient or other data. Finding ways for them to only store limited amounts of data on devices, and to minimize collection of any sensitive data can help lower risks to staff and affected populations. Many mobile data collection tools allow data to be immediately transmitted to the cloud upon hitting 'send', so that data is not stored on a device, and this can help to protect enumerators and frontline staff. In some volatile contexts, organizations have had to keep needs and vulnerability criteria hidden from enumerators as another mechanism of protection. Making decisions about eligibility outside of the country is thought to protect frontline staff from coercion and threats by groups who wish to interfere in the CVA programming or to access data on affected populations.

In addition to the benefits noted above, cloud storage enables access to high levels of computing power, flexibility in terms of the location and flow of data, and cost savings for organizations. It's important to note however, that cloud storage also has its drawbacks in terms of privacy and security. The ICRC identifies two main challenges presented by cloud services: the lack of control over the data; and a lack of transparency about how cloud services process the data. They recommend that humanitarian actors pay particular attention to risks related to: cloud services being accessed from unprotected or insecure locations; interception of sensitive information; weak authentication; data breaches of the cloud service provider; and the potential for access by government and law enforcement authorities. These will need to be assessed and addressed by your security and privacy teams in order to determine how best to manage data responsibly. An additional challenge to consider is that some countries prohibit their citizen's data from being transmitted out of the country, including to cloud servers hosted outside of the country.

More detailed resources on organizational data security and privacy-protecting applications can be found on **this security checklist** and in the ELAN **Tipsheet on Encryption**.

The Centre for Humanitarian Data offers **guidance on data transfers** and **security for organizational operations**.

ICRC provides an **overview of the kinds of data collected automatically** when using digital applications and software. This should be considered when conducting your DPIA, PIA or RBA.

If you are considering storing data in the cloud, don't forget to review national data laws and ensure that data in the cloud is protected through data sharing agreements with cloud hosting providers. Tip: See Chapter 10 of the ICRC **Data Protection Handbook** for a full overview of the use of cloud storage.

USE AND MAINTAIN ROLE-BASED ACCESS LEVELS

Another important way to manage data responsibly is by making sure only authorized persons can access data. For example, an organization might not allow district-level managers to access data at the global level. Enumerators might not be able to access any data in a system; they might only be allowed to upload data into the system. Partners in a large CVA programme might only be able to access the data that they have uploaded but not data that other organizations upload. These role-based permissions should reflect authority and responsibilities in relation to the data concerned, i.e., they should allow access only to the data that different individuals absolutely need to perform their function – no more and no less. Regular reviews should be conducted to monitor data access levels of individuals as they move to different positions within the organization or leave it, as well as consultant and third-party access.

Inbuilt authorization clearances can be set within data management systems, which are triggered requests are made to access certain restricted data. Such safety mechanisms include time stamps, requests to download, viewing tracking, and other kinds of tracking of who is doing what within a database. This helps the IT team or systems manager to continually monitor the security of the database and access to data. It can also help you to determine if the integrity of the data has been compromised or if any kind of fraud or breach is being carried out. Hosting data in the cloud can be more secure in some cases, as this enables laptops and other devices that are prone to theft or hacking to be free of any personal and sensitive data.

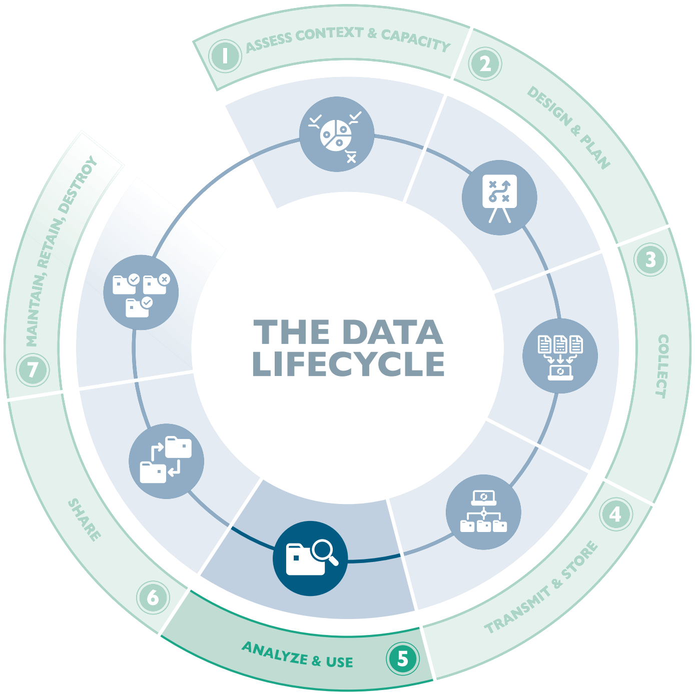
Authorized access levels reduce the possibility of unauthorized data alteration, data leaks and breaches, however, it can be frustrating for organizations that feed data into a larger system if they cannot access the bigger picture by seeing all the data. It may seem that larger agencies are then controlling the data and the power in the response because they have access to all of the data from all partners and thus have more knowledge about trends, which can help them in applications for funding and other partnerships. These kinds of situations might be good to discuss within consortia or the Cash Working Group to find a workable resolution.

Internally, organizations should instruct their human resources teams to draw up data protection and confidentiality agreements for individuals who have access to data to sign, so they are accountable for unauthorized sharing, destruction or misuse of data.

TIP SHEET 5

DATA ANALYSIS AND USE

Once data is available, whether that is new data collected for the CVA response or data from existing sources, it needs to be reviewed for quality and usability. You'll want to review your data analysis processes to ensure that data is inclusive, and that your data analysis does not lead to exclusion of certain individuals or groups from benefits that they are eligible for. If you are using data to make automated decisions, it's important that criteria for and processes of decision-making are clear and transparent, so that they can be reviewed by third parties for bias if there are suspicions or claims that benefits are being allocated unfairly. Additionally, data must be used only for the intended purposes for which it was collected and for which there is consent or another lawful basis for its use.



Tipsheet 5 covers aspects to consider for analysing and using data responsibly in CVA programming.

ONLY USE DATA FOR THE PURPOSE FOR WHICH IT WAS COLLECTED, UNLESS NEW PERMISSIONS ARE OBTAINED

As outlined in Tipsheet 2 (see Boxes 12 and 13 on Lawful Basis), there must be a lawful basis and legitimate purpose for data processing. Before beginning analysis or using data, review the lawful basis under which the data was initially collected, and determine (together with your legal team and data protection officer) whether you are lawfully able to process it.

Humanitarian organizations will often receive programme participant lists for a CVA programme or referrals from other groups (e.g. local partners, colleague agencies, UN bodies or governments). If the data has been collected under the legitimate interest, public task/public interest basis, it may be fine to process it if the secondary processing is along the same lines as what people were originally told about how their data would be used. If the data was collected under a consent basis, you will likely need to obtain new consent before using it for a secondary purpose. It is important to involve your privacy officer or legal team to ensure that you are not violating the law when reusing data.

Financial service providers (FSPs) and MNOs or other private sector entities might want to cross-check lists of beneficiaries or retain metadata for legal purposes, which might be permissible under legal compliance requirements. They might also wish to profile beneficiaries for creditworthiness, which would be incompatible with the original purpose of the data collection (CVA delivery) and require a new lawful basis for data processing, and possibly a new relationship with beneficiaries, with new or additional consent or other permissions. Proceeding with this type of processing would be illegal according to the GDPR, for example. Humanitarian organizations should review any additional data processing by MNOs or FSPs for potential short- or long-term harm to affected populations (for example, future inability to access credit or marketing of exploitative financial service products). This use of data might go against humanitarian principles of neutrality, impartiality and independence.

CLEAN DATA AND CHECK IT FOR QUALITY

Messy data will lead to skewed or invalid results. Whether data is collected directly by your organization or you're using data sets or lists shared by others, data cleaning is needed to ensure data is useful. This might include checking for duplicates, checking participant eligibility criteria and verifying a portion of the list. It will also likely include removing any data that could be used to identify individuals in the data set, unless the data is needed for programme implementation. Be sure to document any gaps, flaws and limitations that are found in the data set(s).

Note: Be careful that you do not inadvertently expose sensitive humanitarian data or information during or after analysis and/or visualization. Analysis of sensitive humanitarian data should only be done in a secure environment and by individuals who are authorized to access the data.

Tip: IMPACT Initiatives offers a **Standard Operating Procedure** for data cleaning that you can use as a guide for your own process.

REMOVE OR DE-IDENTIFY PERSONAL AND SENSITIVE DATA FROM DATA SETS WHERE POSSIBLE

As covered in Tipsheet 3, Data Minimization is a core principle of responsible data management. One way to minimize the amount of personal or sensitive data that you are holding is to de-identify it. In other words, to remove identifying information so that the data becomes 'anonymous'. When data is anonymized or de-identified, the association between data and the individuals to which it relates is removed so that an individual cannot be identified in the data. This is done by removing both 'direct identifiers' and 'indirect identifiers', for example, by removing a national ID number or a birthdate. This process makes the data more private and puts people at less risk because it has been scrubbed of identifying information or aggregated to a level where individuals cannot be identified.

It's important to remember that even de-identified or aggregated data can put entire groups of people at risk – for example, if the location of particular ethnic or religious groups could be used to attack those groups. If information is released about where a CVA distribution is going to happen or has happened, this could result in unwanted groups interfering with or harming individuals who are receiving CVA or organizations that are providing it. Besides firstly planning how to anonymize or de-identify individual data, you will need to also consider how to protect non-personal data. Certain data should only be shared or released to those who need it for approved purposes and in suitably protected data environments with appropriate technical and organizational controls.

Because technology and data analytics is becoming ever more sophisticated, you will likely need support from your data or IT team for data de-identification.

Anonymized data is safer, but if it is too generalized, then it becomes useless for delivering CVA. You'll need to find ways to minimize data yet still achieve your CVA aims.

Even if individual-level data has been de-identified, individuals might be re-identified through (statistical) matching with other data sets or within individual survey results. CVA lists are often combined and merged, both inside individual organizations and after data sets are shared. If this is the case, it becomes easier to identify individuals within data sets. Statistical Disclosure Control is one method to assess the risk of reidentification and reduce it before sharing data. OCHA **provides guidance** on this method.

When collaborating with commercial partners in locations where there are concerns about data privacy, one option might be to establish an agreement with one FSP to use sub-accounts, whereby the due diligence or KYC is completed only on the implementing agency as the main account holder, and not on those accessing the sub-accounts. Sub-accounts can be accessed through smart cards (e.g. pre-paid or ATM cards) that only have reference numbers attached to them, and do not include personal details. Cash recipients are then able to withdraw cash without their personal data being shared with the FSP. Only the implementing agency has the information that links the card or account to the cash recipient.

AUTOMATED DECISION-MAKING

The UN Special Rapporteur on extreme poverty and human rights warned in 2019 that welfare reforms facilitated, justified and shielded by new digital technologies can reflect values and assumptions that are not aligned with human rights principles.[37] For example, individuals can be mistakenly excluded from benefits when decisions are made by automated software programs. Additionally, people can be permanently flagged or categorized in ways that can lead to future discrimination, e.g., someone who received benefits due to their refugee status during a particular phase of their life might be permanently flagged by decision-making algorithms as a credit risk. As CVA programming becomes increasingly digital, it is important that humanitarian values remain at the forefront and that data harms and exclusion are not exacerbated by the digital tools and technology that CVA actors incorporate into their programming. Automated decision-making (ADM) on the basis of data may allow for greater scale and more rapid decision-making, but this is still in the early stages and could lead to exclusion or future harms.

The GDPR also contains specific articles that protect individuals whose data is subjected to automated decision-making that has legal or similarly significant effects on them. The GDPR mandates, for example, that if conducting this type of decision-making, individuals must have information about the processing; there must be simple ways for them to request human intervention or challenge a decision; and you must carry out regular checks to make sure that your systems are working as intended.

While most organizations are not using ADM in their programming, it is increasingly being used in the commercial sector for financial transactions such as credit approvals. In the context of CVA, some organizations are working out how to use call detail records (CDRs) to target potential cash recipients.

If used, automated decision-making should be in support of human decision-making, not in place of it. CVA organizations should ensure that any ADM used for targeting or enrolment and registration is carried out with open and transparent algorithms, human oversight, comparative research and testing to check potential biases, and clear mechanisms for complaints and redress if decisions are erroneous or lead to future harms.

See the CaLP **Case Study on Remote Targeting using Non-Traditional Data** for more discussion on this topic.

[37] Alston, P. (2019) 'Report of the Special Rapporteur on extreme poverty and human rights'. UN General Assembly.

TIP SHEET 6

DATA SHARING

CVA actors work in a wide variety of contexts, including active conflicts, refugee crises, instances of internally displaced populations and blockades. Data sharing is necessary in CVA programming, and as Cash Working Groups and consortia align and collaborate, partnerships are established with FSPs and Mobile Network Operators (MNOs), and social protection linkages are made, data sharing is happening more frequently for coordination and other reasons.

Donors and humanitarian actors increasingly support the development of single or social registries for social assistance programmes and greater interoperability and information sharing, and to move away from separate and disconnected management information systems (MIS). Some UN agencies, for example, the WFP, UNHCR, UNICEF and OCHA, are pushing for common approaches to humanitarian CVA and collaboration among agencies.[38] However, the benefits of data sharing are often defined in terms of efficiency gains, with little reference to protection and other advantages and trade-offs.[39]

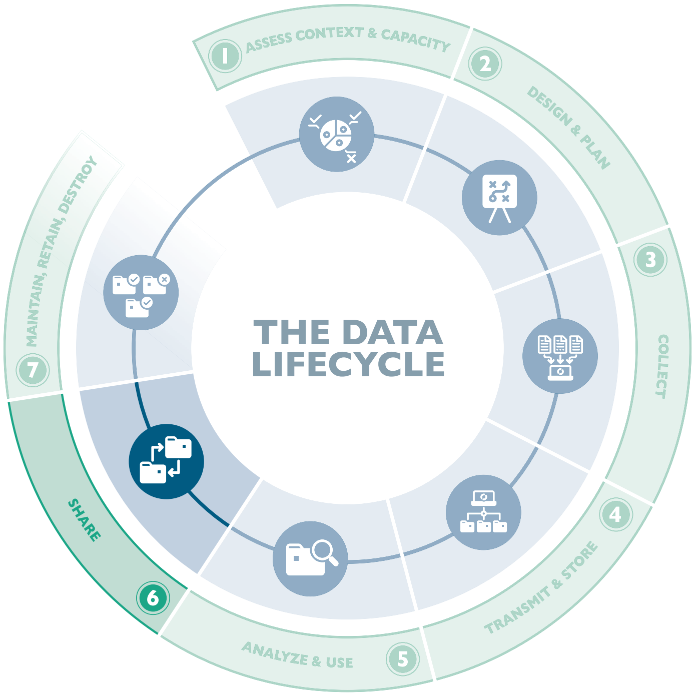
DETERMINE WHAT INFORMATION NEEDS TO BE SHARED, WITH WHOM, AND WHY

As outlined in Tipsheet 2, Box 10 on data controller(s) and data processors, data controllers make decisions about how data is collected and processed. They also make decisions about data sharing. Data processors should not make decisions about who and why data can be shared, this should be the mandate of the data controller. [40]

Before sharing any data, you should determine the following parameters:

- **Purpose:** Why are you sharing? What data are you sharing? Do you need to share all of it to achieve the purpose or can you just share part of it or certain fields?

- **Legality:** Are you legally able to share this data or to decide that it should be shared? Do you have permission and/or have affected populations been informed that it will be shared?



Tipsheet 6 provides guidance on responsible data sharing, while recognizing that this is a contentious area that will need to be worked out on a case-by-cases basis, depending on context and the actors involved.

[38] See this announcement about the Common Cash System.
[39] Goodman, R. et al. (2020) 'Review and Analysis of Identification and Registration Systems in Protracted and Recurrent Crises'.
[40] Information Commissioner's Office of the UK (2018) 'Controllers and Processors'.

- **Mechanics:** How will you share it? How will it be stored? Have you vetted the organization with whom you will share the data to ensure they can keep it secure and private? (See Tipsheet 4 on Data Transmission and Storage)
- **Description:** Have you provided sufficient description of the data and context in which it was collected, when it was collected, and other key information so that data is not used out of context?[41]

You will probably need to create different versions of data sets for different uses and partners. Personal and sensitive data should only be shared if it's absolutely necessary and after there is a data sharing agreement in place.

Prior to sharing any kind of data, it is essential that you ensure that people reflected in the data understand what will happen to their data and have either given their informed consent for its use or that another lawful basis for data processing and sharing has been established. This means that participants have given their permission for the data to be shared, with full knowledge of the potential consequences (see Tipsheet 2 and Boxes 12 and 13).

Access to personal and sensitive data should be on a 'need to know' basis, not the default.

Consider what kind of access partners actually need and, if possible, set access permissions and database trackers to control who can view, add, alter, download or delete data.

ASSESS RISKS AND BENEFITS BEFORE SHARING DATA WITH GOVERNMENTS

There is a commonly held assumption that centralized humanitarian CVA systems will form the basis of longer-term or government-led social protection systems. These assumptions should be weighed with aspects of privacy and data protection because of potential effects on fundamental rights of beneficiaries.[42] In some cases, a single system may be the right option, and in others, the context of the country and the response might mean that this is not ideal. In any context, organizations should try to assess this jointly to find the best solution for crisis-affected populations.

Data sharing with governments, depending on the context, can carry high risks for vulnerable populations; for example, if irregular migrant data were shared with governments that do not welcome migrants, or data from refugees or internally displaced populations were accessed by local armed groups who wish to do them harm. In addition to legal (yet potentially harmful) data sharing, forced data sharing happens at various levels of a response, including at the local level when enumerators are threatened and harassed, and at higher levels where agencies feel pressure to share data in order to be allowed to operate in a country or a particular zone of a country. It is also important to remember that data that is shared with one part of government might then be shared further with another part of government, and that data shared with entities which are mandated to share with governments may be obliged to share onward the data that you collect.

Remember that governments change, and so data sharing that may appear to be unproblematic today might not be so next year. For this reason, data minimization and limited data sharing is a best practice, as noted in Tipsheet 2, where we talk about data governance. A change in government should act as a trigger for reviewing and potentially updating your DPIA.

See the CaLP **Case Study on Data Sharing with Governments**.

ASSESS THE RISKS AND BENEFITS OF DATA SHARING AND COLLABORATION WITHIN A CONSORTIUM OR CWG

If conducted well and with sufficient attention to data protection, data sharing and the use of common and interoperable systems can facilitate the CVA implementation process and reduce duplication and fraud. Establishing Information Sharing Protocols (ISP) at the response-level (via the ICCM or HCT), for example, is recommended in the IASC Operational Guidance on Data Responsibility. The establishment of a CWG-specific ISP in contexts where this is useful is also recommended. At the same time, because data is power, there are often challenges within consortia or CWGs when determining which system to use and who accesses and manages the data within the system. Additionally, single systems and increased data sharing can expose CVA recipient data to privacy violations as well as direct harm if data is breached or shared with actors who misuse it.

[41] Doornbos, A. (2020) 'Data Sharing with Partners'.
[42] Goodman, R. et al. (2020) 'Review and Analysis of Identification and Registration Systems in Protracted and Recurrent Crises'.

Consortia and/or CWG members often experience challenges collaborating and sharing data with one another. As noted in Tipsheet 1 on context and capacity, the process of determining who leads a response and who shares data with whom is fraught with tensions related to power and control of a response, current and future access to donor funding, and different approaches and concerns regarding the privacy of CVA recipients. Some organizations express reservations about how much data is captured from CVA recipients, whether that includes biometrics, and whether data systems managed by other actors are sufficiently secure. Moreover, those implementing partners that are funded by the UN may have to share data with UN agencies in order to participate in a response. Clearly, tensions exist when the provision of funding is dependent on data sharing arrangements, because provision of, access to and control of data is political and involves power dynamics.

While each organization will have its own systems, if data sharing is part of the CVA response, data will need to be interoperable so that it can feed into the same information management system. This is another challenging aspect of data sharing – agreeing what data should be collected and how it should be structured so that it can be effectively used.

Some CVA actors, consortia and CWGs are innovating with different ways to share data within established data sharing agreements. For example, if organizations don't have data sharing agreements with each other, but they each have a data sharing agreement with a third agency, they might decide to each share data with the third agency, which can then serve as a link, while remaining within legal and data sharing agreements. Other CWG members are experimenting with different ways to anonymously share data, for example, through a secure 'hash' or using the blockchain. Turkey's Emergency Social Safety Net programme has developed a shared information architecture for data across partners, and to align information systems without sharing data with all actors. CVA actors can also establish information sharing protocols (ISPs) or standard operating procedures (SOPs) that guide how data can be shared between or among agencies.

Data protection law can be used to further decisions about data management. Data controllers will bear the responsibility if there are data breaches or other privacy violations, and the controller is responsible for managing any accountability-related requests from affected populations. By establishing who is the data controller and who is the data processor, or if there will be joint controllers, organizations may be able to find a neutral ground under which to have an open discussion relating to power and accountability (see Tipsheet 2, Boxes 10 and 11 on data controllers and data processors).

REVIEW FSP AND OTHER THIRD-PARTY DATA POLICIES BEFORE AGREEING TO SHARE DATA

As cash modalities have shifted to include more FSP and MNOs, CVA actors frequently share programme participants' personal data with FSPs and host country governments to meet KYC and other requirements. This data may include names, telephone numbers or ID numbers, as well as, increasingly, biometric data. FSPs often hold transaction records in addition to personal data. These provide a record of where and when people make purchases and information about savings and spending. This transaction data should be protected from misuse. It is important for CVA actors to have a clear picture of what data FSPs will gather about programme participants while providing their services and to assess, during the DPIA or RBA process, the potential risks this could pose to affected populations. There should be explicit data sharing conditions in any contracts, as well as stipulations related to responsibility for any kind of data leak or breach.

When setting up agreements to share data with private sector partners, including FSPs and MNOs, make sure that you review their data sharing policies and terms and conditions and include robust conditions in your own agreement to ensure the appropriate standard for data protection and data responsibility more broadly, including restrictions on forward sharing, use, retention and destruction. Some may include a default clause within their contracts, allowing 'sharing with third party', meaning that they can share any data with anyone in the future. Such providers will likely also have a clause stating that if they are acquired or sold, any data they hold will be a key part of the assets that will be included in the sale or acquisition.

If you are not comfortable with this scenario, make sure to raise the issue in advance of data sharing or agreeing on a partnership. It may be perfectly reasonable to push back against a default data sharing policy and make access to CVA programme data more considered and tailored to the particular needs of the third party.

Due diligence assessments should be conducted on private sector partners before any data is shared.

FSPs and other third parties may push back on restrictions related to data sharing and further use. In some cases, they may have legitimate reasons (for example, if they legally need to provide KYC or other data to governments). In others, they may have a business model that is based on profiting from data, and this may be incompatible with the humanitarian mission. While legal requirements such as KYC are non-negotiable, it is possible to add clauses that prohibit the use of CVA recipient data for marketing purposes or to stipulate that FSPs must be transparent and must notify organizations when there is a request for data sharing with government authorities.

Colleague agencies may not be aware of data sharing risks, so it's important to have a discussion about this prior to signing data sharing agreements.

ESTABLISH DATA SHARING AGREEMENTS BEFORE SHARING ANY DATA

Before sharing data, it is important to explicitly state what type of things can or cannot be done with data. This is normally done through a data sharing agreement. Data sharing agreements do not necessarily contain information specific to the programme data you will collecting. Rather, they make explicit the 'dos and don'ts' that might arise when sharing data. They should include minimum standards for data security and privacy and establish responsibilities and liability for data privacy violations and for security breaches or data misuse, or forward sharing without authorization.

It can take several months to establish a data sharing agreement, even if there are existing terms of reference for cooperation among organizations and agencies. This is in part because it takes time to establish interoperability standards. It is also because organizations and agencies usually need to involve their legal, data protection and IT teams, which may require both country- and global-level engagement for international organizations. While there has been a tendency to share data without having an agreement in place, it should be noted that Data Sharing Agreements and Data Transfer Agreements are required by law under the GDPR and other data privacy regulations. In some cases, negotiating data sharing agreements has become an exercise in power by larger organizations over smaller ones.

Information about data sharing must be included in the consent requests or other information that is provided to affected populations so that they are clear what they are consenting to or what will happen with their data. Even if you do not use 'consent' as your lawful basis for data collection, you must transparently inform people about any parties with whom you would share their data.

In cases where an urgent response needs to be carried out and a data sharing agreement has not yet been worked out, you might need to share a limited amount of data under a focused and time-bound MoU so that you can proceed with the response. This is a trade-off to consider. Is it better to share data so that the response can proceed, or is the risk too high? In these cases, you might want to go with the least data-heavy CVA programme design that you can manage.

Data sharing agreements are an important tool for responsible data management. In practice, however, accountability mechanisms for these agreements might be difficult to implement, meaning that there is little control over how data is used or shared further. For this reason, it is important to adhere to data minimization principles when determining exactly what data needs to be shared and with whom.

Data sharing among CWG members and consortia, with governments and with FSPs should be a key area to assess when conducting your DPIA, PIA or RBA at early context and capacity assessments and during programme design and planning. You should also do background research to ascertain data protection levels operating during past responses and data systems that are being proposed for a joint response.

The UNHCR and WFP have developed a Data Sharing MoU, available **here**.

OCHA's **Data Responsibility Guide** covers the topic of data sharing.

STRATEGIZE AND REHEARSE PREVENTION AND RESPONSE TO 'FORCED DATA SHARING' AND OTHER CRITICAL DATA INCIDENTS

In addition to agreed data sharing, in many CVA programme contexts, 'forced data sharing' is a reality. Your staff and local partners might be coerced by various means into sharing data with groups who stand to gain from data access and control. There are also concerns that some entities share data that should not be shared, such as when some organizations are unwilling to share data with governments, yet the data is obtained via FSPs or another partner agency. It is important to identify potential risk areas for forced data sharing and to rehearse how you and your staff might respond.

See Tipsheet 2, Design and Planning, for more on critical data incidents.

CaLP is encouraging Cash Working Groups and consortia to collaborate and jointly strategize on how to respond to common data incidents in their contexts, and to contribute to a registry of these incidents so that more research and learning on good practices can be done. See the **CaLP Critical Data Incident Management initiative** for more information.

OPERATIONALIZE YOUR DATA SHARING AGREEMENTS

It is one thing to draft data sharing agreements, and another thing to ensure that they are implemented. Organizations should ensure that their staff and partners are aware of what is contained in data sharing and other data-related agreements with donors, governments and FSPs so that organizations will not share or otherwise manage data outside of these agreements, and so that partners will abide by that which is agreed.

Data sharing agreements take a good deal of time and effort, and they can be difficult to work out. They will require sign-offs from legal teams and data protection offices, which can entail considerable review stages. It is important to develop data sharing agreements as one of your first tasks in the response, and to resource this process so that the necessary staff and time are in place from the outset.

Set up a time to review agreements with partners and discuss data management expectations and data sharing restrictions early in the process. Provide training if needed. You may need to provide capacity support or other resources to partners if they require improved skills, knowledge or systems in order to implement and fulfil requirements for safe and responsible data sharing.

TIP SHEET 7

DATA MAINTENANCE, RETENTION AND DESTRUCTION

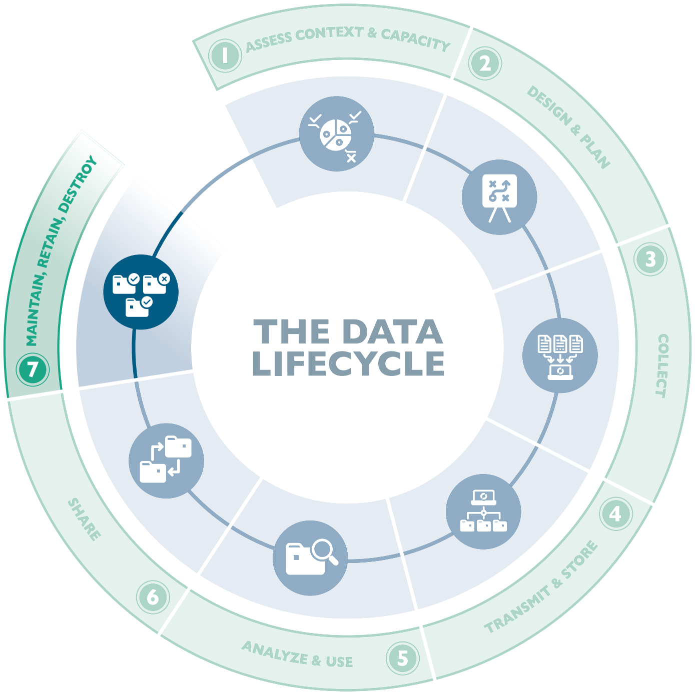
Throughout the programme cycle, data that you collect will need to be safely stored and kept secure, as noted in Tipsheet 4. When a response is complete, data will need to be retained or destroyed, depending on the situation. Your organization should retain personal and sensitive data only for as long as necessary. In general, the sooner that personal data can be anonymized or aggregated, the better. Once data is no longer required for legal or other legitimate purposes, you should securely destroy it.

PLAN AND BUDGET FOR DATA MAINTENANCE, RETENTION AND DESTRUCTION FROM THE OUTSET

While data retention and destruction happen at the end of the programme or end of the data lifecycle, you'll need to have planned for them in the early stages of design and planning to ensure sufficient budget. Lack of planning can put programme participants at risk or cause you to store data longer than necessary. In order to plan properly you'll need to understand the needs of all stakeholders. Even within the same programme, different teams might have different data retention needs. For example, finance and compliance staff might need to access programme data for a donor audit years after a programme ends. In contrast, programme staff may no longer need data once the programme is complete. To meet the data needs of all teams, it is important to reach a shared understanding of each team's data retention needs prior to programme end and to ensure that the systems used for collecting and storing programme data will coordinate smoothly from start to finish.

ONLY RETAIN THE DATA THAT YOU NEED, AT THE LEVEL OF GRANULARITY THAT YOU NEED, AND DESTROY THE REST

CVA programmes gather a lot of data. Depending upon your programme type and funding structure, you may need to retain relevant data to justify decision-making, for audit purposes, or for monitoring, evaluation and learning purposes. Programme managers may be afraid to delete data for fear of deleting something important. And while this can



Tipsheet 7 provides guidance on responsible data retention and destruction.

(Tipsheet 4 on Transmission and Storage provides more information on securing data for an active response.)

be a risk, keeping data for too long is a risk, too. The more personal and sensitive data that is held, the more liability and greater risk an organization assumes, and the higher the risk for CVA recipients that their data might be leaked or accessed by those who may misuse it or do them harm. Additionally, as time goes by and staff change, it becomes increasingly difficult to ensure that data is accurate, that new staff are aware of the limitations set on a certain data set, and that a data source and permissions associated with it can be accurately traced. What's more, an organization holding data is responsible for that data, and it must be able to respond to requests from participants to access their personal data. The more data an organization holds, the more difficult this becomes.

Your organization may already have an overall data retention policy, and it should include your CVA data. If you are working in a wider consortium, a data retention policy should be agreed upon with members. The Cash Working Group may be a good place to discuss at what point in the CVA programme cycle certain data should be aggregated and what are the right time frames for destruction of specific kinds of data. You will want to set clear terms for data retention and destruction in your various guiding documents, MoUs, data transfer and data sharing agreements, etc.

While it can be tempting to keep lists of CVA recipients for extended periods, they will lose their relevance after a time, and will no longer be useful for cash targeting and distribution if they are not maintained and updated.

A Data Retention plan is sometimes referred to as a Retention, Archival and Destruction (RAD) plan. See the ELAN **Data Starter Kit** tipsheet for more guidance and examples of a RAD.

CaLP
The Cash Learning Partnership

german
humanitarian
assistance
DEUTSCHE HUMANITÄRE HILFE

www.calpnetwork.org

March 2021