Data sharing in humanitarian Cash and Voucher Assistance (CVA): A look at risks, threats and mitigation technologies

Published 2023-11-28

NRC NORWEGIAN REFUGEE COUNCIL

THE ENGINE ROOM

Acknowledgements

Written by: The Engine Room (https://theengineroom.org)
Owner: Tariq Riebl, Global Programme Strategy and Innovation Director
Approved by: Frédéric Gibaudan, Research Lead Consultant
Updated: 23/11/2023
Cover photo: NRC team talking to the families that have been displaced to the collective shelters to assess their needs after the earthquake, Aleppo, Syria. (Credit: Tareq Mnadili)

Norwegian Refugee Council
Prinsens gate 2
N-0152 Oslo
Norway

www.nrc.no

Research lead: Quito Tsui (The Engine Room)
Research: Olivia Johnson (The Engine Room)
Technical evaluation: Wouter Lueks, PhD (CISPA)
Writing: Quito Tsui, Olivia Johnson, Wouter Lueks and Helen Kilbey
Editing: Helen Kilbey
Review: Frederic Gibaudan (NRC), Thomas Raffort (IFRC)
Design & layout: NRC

Funded by European Union Humanitarian Aid

This research and publication were made possible thanks to funding from the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

We want to thank all of the people who generously shared their experiences and ideas with us in interviews.

This report is based on research commissioned by the Norwegian Refugee Council (NRC) in collaboration with the members of the Dignified Identities in Cash Assistance consortium (DIGID), the International Federation of Red Cross and Red Crescent Societies (IFRC), the Norwegian Red Cross and Save the Children Norway, and was conducted by The Engine Room from March to October 2023.

Suggested Citation: The Engine Room: Q Tsui, O Johnson, H Kilbey. CISPA: W Lueks (2023). Data Sharing in Humanitarian CVA.

TABLE OF CONTENTS

How to read this report

- **Section1: Introduction** explains the background context for this research, including aims, audience, scope, limitations and research methodology. It also includes a set of key observations that surfaced in our interviews and desk research. >> *This section offers important context for the rest of the report.*
- **Section 2: A snapshot of data sharing in CVA** lays groundwork by mapping out key elements to take into account, including stakeholders, data flows, data types, and policies and guidance that govern sharing. It also presents some of the technical tools currently used for sharing data. >> *Readers who are already familiar with the humanitarian CVA data environment may want to skim this section in order to move more quickly to Section 3.*
- **Section 3: Areas of potential risk & harm and challenges to protecting data in humanitarian CVA contexts** builds on Section 2 by analysing relevant risks and threats, including basic underlying risks, stakeholder-specific risks, and specific challenges that the CVA ecosystem presents for data security. It also includes discussion on potential harms to people receiving assistance. >> *This section is the heart of this report, and includes discussion of risks and harms that are relevant to any humanitarian practitioner who works with data in some capacity.*
- **Annex: Relevant technical approaches to risk mitigation and how to evaluate these in context** This section is more technical than the rest, and takes a close look at potential technical mitigation approaches. >> *The Annex was written primarily for decision-makers in the CV data ecosystem, but will also be relevant to anyone wishing to better understand how to start building technical systems that incorporate security and privacy by design, and anyone wanting to gain more understanding around emerging cryptographic and other relevant technical approaches and terminology.*

Section 1: Introduction

In recent years, both the rate and extent of data collection in the humanitarian sector has increased. At the same time, scrutiny and sectoral discussion of data-sharing processes has also grown, as humanitarian organisations reflect on the potential risks involved in sharing the data of vulnerable individuals.[1]

This discussion is especially relevant in the case of Cash and Voucher Assistance (CVA) programming, where clustered approaches to humanitarian operations along with the digitalisation of CVA programming following the pandemic[2] has resulted in large quantities of CVA-specific data being collected by humanitarian organisations in a data sharing ecosystem that can include a range of actors – from partner organisations and host governments to financial and other service providers.

This complexity, alongside an **absence of robust standards** for sectoral data protection and responsible data sharing, introduces **new and amplified risks** to the communities humanitarian organisations work with: **each node that is added** to the data ecosystem – be it humanitarian

[1] e.g.” Why Data Protection is Critical in Humanitarian Action,” Red Cross Red Crescent Magazine, January 27, 2021, https://www.rcrcmagazine.org/2021/01/data-protection-critical-humanitarian-action/.

[2] The Centre for Humanitarian Data, “Data Responsibility in Cash and Voucher Assistance,” OCHA, (December 2020), https://www.alnap.org/help-library/data-responsibility-in-cash-and-voucher-assistance

partners, host governments or private sector vendors – brings additional potential weak spots that must be assessed for the ways in which they may introduce added risk.

Research aims, audience, scope & limitations

Against this background, this research, conducted by The Engine Room between March and October 2023, was commissioned by the Norwegian Refugee Council in collaboration with the DIGID consortium to map risks and threats related to data sharing in CVA, and to evaluate potential technological approaches that might mitigate these risks. The research forms part of a broader initiative focused on interoperability and data sharing in the humanitarian sector.

This report aims to support decision-makers involved in considering, evaluating or building new technological approaches to data sharing in CVA. It should however, be of interest to many others working in humanitarian CVA, as it covers important topics that are relevant to anyone who handles data in the course of their humanitarian work. As such, we hope that it will find its way to a broader audience.

The research had two main aims:

1. Analyse risks and threats related to data sharing in CVA, taking into account a landscape scan conducted by the DIGID consortium that identified key use cases.[3]
2. Evaluate potential technologies for mitigating these risks, as identified by interviewees as well as by parallel research commissioned by DIGID consortium and conducted by Caribou Digital.[4]

Risk, however, tends to be **highly context-specific**: risk assessments and threat modelling are usually applied to specific systems and contexts, whether projected or actual. As humanitarian CVA contexts are complex and varied, and the data-sharing use cases that were the starting point for this research were fairly generalised, there were **natural limitations** to the kind of risk and threat analysis that could be done.

With this in mind, the research surfaced a set of key risk areas to consider when looking at data sharing in CVA. These can be used to inform data-related safety by design in subsequent work, and to guide risk and threat analysis in more contextually-specific scenarios.

In aiming to evaluate how well a set of identified technological approaches might be able to mitigate these risks, similar limitations arose. Data protection and security involve many factors, and technical tools and protocols are just one part of the overall ecosystem. How well or how little a technical system protects data will depend on the details of the full ecosystem and the context the technology operates within, as well as the finer details of how it is set up and deployed, how well it can be maintained, and so on.

Here, too, this report offers guidance for future, more context-specific work by offering decision-makers an overview and explanation of some of the mitigation technologies that surfaced, and by presenting key questions that should be asked in the context of specific deployments.

These are designed to **support decision-makers** to better understand and determine how much protection that technology is likely to be able to provide in a given context – or whether it's even feasible to deploy in the first place. (It should be noted here that technical security expertise will still likely be needed for this kind of contextual evaluation).

[3] Robert Worthington and Andrea Duechting, "Enabling Dignified Humanitarian Assistance Through Safe Data Sharing," IFRC, (2023), https://static1.squarespace.com/static/639843c19e367d3f019f26f6/t/64615d026ec1c54e3020066d/1684102440772/DIGID+Interoperability+-+Landscape+Mapping+Overview.pdf.

[4] Caribou Digital, "Investigating Safe Data Sharing and Systems Interoperability in Humanitarian Cash Assistance," IFRC, (2023), https://static1.squarespace.com/static/639843c19e367d3f019f26f6/t/6540f33fa9b72003914ad695/1698755414564/DIGID+Interoperability+-+Investigating+Safe+Data+Sharing+and+Systems+Interoperability.pdf.

Methodology

The research for this report was conducted primarily through desk research and interviews.

An initial desk review scoped out the current state of CVA data-sharing, including CVA data flows, evidence of intrusion, risk and threats of CVA data-sharing and potential technological mitigation and protection measures. Throughout this phase we identified key individuals to interview.

In interviews, we selected ten individuals with a combination of deep sectoral and cybersecurity experience, who had technical experience of data sharing and data protection in the humanitarian sector. Our interviewees were split across three main cohorts:

- Humanitarian agencies
- Privacy and Digital Rights organisations
- Researchers and research centres working on cybersecurity
- The interviews were semi-structured and designed to capture a detailed picture of CVA data sharing, including:
- The organisations, data type and platforms involved
- Current challenges
- Risks associated with data sharing, including human rights, technical, legal and operational concerns
- What tools and technical processes are being used or considered to manage and mitigate risk.

The research team then coded interview transcripts to generate patterns and identify key findings, to inform and complement the desk research.

All interviewees have been kept anonymous, to allow them to speak openly.

Key observations

Our research surfaced not just a picture of risk in humanitarian CVA generally, but also questions around interoperability as a goal for the humanitarian sector more broadly. We found that:

- **Interoperability is contested as a goal for the sector.** In interviews there was a **lack of agreement** on whether the current extent of data shared for CVA can properly be justified given the potential risks and harms involved in doing so, and a lack of agreement on whether interoperability should be a goal for the sector in the first place.
- **Tensions** around interoperability have also been reported between UN agencies and among some implementing partners, as WFP, UNHCR and UNICEF have started working on ways to make their systems interoperable with one another as well as with governments. Concerns raised include data protection and security, and power imbalances, specifically concerning UN requirements, privileges and immunities.[5] This points to a need to reflect on interoperability as a necessary goal for humanitarian programming.
- There's a lack of agreement when it comes to need vs risk. Security is ultimately a dynamic conversation about need vs risk – in other words, whether the need or desire to do something can be justified when weighed against the risks involved in doing so.

[5] Linda Raftree, "Data Responsibility Toolkit: A Guide for Cash and Voucher Practioners," CALP Network, (March 2021): 13, https://www.calpnetwork.org/wp-content/uploads/2021/03/Data-Responsibility-Toolkit_A-guide-for-Cash-and-Voucher-Practitioners.pdf.

- It follows that sector-wide decisions about risk mitigation will require some agreement on the acceptable level of potential harm that can be justified for each data-sharing use case, when weighed up against potential benefits.
- In interviews, the acceptable **need/risk ratio** of the specific interoperability use cases we looked at was contested – an information management expert at a humanitarian organisation we spoke to, for example, questioned fraud prevention as a justifiable reason to collect and share data, both from a resource management perspective and from a risk perspective:

  > "How much money are we [trying to save by] finding these people who are trying to trick the system versus how much we are paying for those systems and trying to set it up? I'm much more about collecting way less data than we need and if we see that there is huge risk in wasting resources and so on, then put the protection of the refugees first and try to sort out how we do the assistance in the easiest way possible."[6]

- There is a need to establish shared data protection standards grounded in deployment contexts. Information is only as secure as the "weakest link" in the system – meaning that if information is available or accessible in many places, to protect this information you need to protect each of these places equally well. Without shared standards it is difficult for humanitarian organisations to ascertain the baseline data protection measures being taken by peer organisations.
- Risk mitigation is multi-faceted. No single technical approach alone will be able to fully mitigate risk – rather, risk mitigation necessarily involves a combination of technical approaches and specific actions, and is a dynamic process that requires careful consideration of both data protection systems as a whole and the individual constituent parts that comprise the overall system. As a result, each context has specific needs and risks that will need to be considered both in the overall design of any data protection system, and when choosing individual technical components.
- Once data is shared, protection cannot be guaranteed. At a basic level, data, when shared, can never be protected from those with whom it is shared. Risks associated with data sharing cannot, therefore, be fully mitigated, meaning organisations should assume data will be breached in the process of data sharing. This will be an important assumption to keep in mind when evaluating or designing systems for sharing data.
- **There is interest in alternative approaches.** Some of those we interviewed encouraged the sector to look to other approaches, including more purpose-limited methods that consider what needs at base to be achieved, and how that can be done *without* sharing data. Some examples of these kinds of purpose-limited solutions are discussed in the Annex.

[6] Interview with information management expert at humanitarian organisation

Section 2: A snapshot of data sharing in CVA

In order to understand the risks involved in data sharing in CVA, and to evaluate potential ways to mitigate that risk, it is necessary to first have an **understanding of the key elements involved, and to have some insight into the current landscape.** With this in mind, this section maps out the key stakeholders, data flows and types, use cases for sharing, policies and guidance that currently govern sharing, and technical tools that surfaced in our research.

As mentioned earlier, those readers who are already familiar with humanitarian data flows may want to skim this section in order to more quickly get to Section 3: Areas of potential risk & harm, and challenges to protecting data in humanitarian CVA contexts.

Primary use cases for data sharing in CVA

The IFRC's landscape mapping report[7] identified four main use cases for data sharing in CVA: **deduplication**, **organisational and individual referral**, and **vertical integration** (sharing data on a

[7] Worthington and Duechting, "Enabling Dignified Humanitarian Assistance."

person with a payments or messaging provider). Our own research found that humanitarian data might also be shared for **monitoring and auditing** purposes, and for **legal compliance**.

It should be noted that in our research, some interviewees questioned whether all of these use cases were actually necessary – particularly when it came to deduplication. Multiple interviewees said that, given the inherent risks involved in sharing data about people receiving humanitarian assistance, **resources should be put towards** addressing underlying issues rather than interoperability. Two issues in particular were brought up in interviews:

1. **Multiple organisations operating in the same context,** and a lack of effective coordination between them. More than one interviewee noted the complications brought about by multiple humanitarian actors operating in the same space,[8] resulting in different organisations collecting similar data on overlapping populations.

2. **Lack of trust between organisations operating in the same context**: an expert on humanitarian operations we spoke to talked about what they saw as a lack of trust between organisations working in the sector, which leads to organisations wanting to own their own data, leading to multiple databases housing similar or duplicate data.[9]

Relevant stakeholders in CVA data sharing

In the context of risk, stakeholders in CVA data can be understood to include not just entities that might have direct contact with data, but also those who have an interest in obtaining it. One data expert we spoke to summed up some of this complexity:

> "Who are all the people involved? From people at the registration desk to people in the headquarters, people in different departments, doing audits, distribution – from different people who get data upstream, to governments to paramilitary groups."[10]

Given this, any context-specific risk analysis should be careful to look at the full spectrum of stakeholders (both actual and potential). In general terms, however, the main stakeholders in data sharing for CVA are **humanitarian organisations** (including UN organisations), **donors** (in humanitarian CVA this is primarily governments, but private actors also play a role), **host governments**, **local NGOs, financial service providers (FSPs)**, and **third-party software and hosting providers**.[11] Occasionally, third parties like **academic institutions** or **consultants**, with whom data is sometimes shared for research purposes.[12]

As each of these broad groups contain wide variety within them, in any context-specific risk analysis it will be important to look at each stakeholder individually, as well as to take into account any power relations between stakeholders.

[8] Interview with digital security expert at humanitarian organisation

[9] Interview with expert on humanitarian operations

[10] Interview with digital security and privacy researcher

[11] Raftree, "Data Responsibility Toolkit."

[12] Interview with data protection expert at humanitarian organisation; Interview with privacy expert and advocate; Interview with data privacy and legal expert at humanitarian organisation

Mapping out CVA data flows and data types

Data flows

Understanding what kinds of data is shared between organisations is crucial for identifying the possible risks associated with each form of data, and having an accurate and detailed map of data flows situated in a specific context is needed for informed risk assessment.

Detailed data flows for the sector as a whole are difficult to map out, as these vary widely and are also generally not made publicly available; our research also showed that data is shared in both formal and informal ways in practice, and as such can be ad-hoc and very dependent on context.

As a basis for understanding risk on a higher level, however, a CVA data flow might follow the following stages: **Targeting or needs assessment > registration > delivery > monitoring & evaluation.**

Data types

At the heart of data protection in humanitarian CVA is the information humanitarian organisations collect on those receiving assistance. This can include:

- **Directly identifying personal data** such as name, family name, ID number, phone number, address, bank details. CVA is also increasingly utilising the collection and sharing of data from digital ID systems and biometrics (iris, voice, fingerprints, facial imaging) for identification and verification purposes.[13] [14]
- **Data related to certain characteristics** such as disability, gender, sexuality, ethnicity, religious affiliation, social affiliation, and political affiliations.[15]
- **Aggregated data** from needs assessments, feedback surveys or larger datasets (for example, showing the number of people reached by a particular service).[16]
- **Metadata** such as data about transactions (e.g. withdrawals) and spending.[17]
- **Location or movement data** such as movement between refugee camps (collected especially when communities interact with humanitarian organisations repeatedly over time)
- **Data related to referral information** like past services received or previous requests made for services.[18]

There is **wide variation in how/how much data is shared in humanitarian CVA contexts**. Some organisations share very little data in a controlled way, while others can be more on the "buffet side of the spectrum" as one digital rights expert put it, sharing data more indiscriminately and

[13] The Engine Room: Tsui, Q., Perosa, T., and Singler, S., "Biometrics in the Humanitarian Sector," (July 2023), https://www.theengineroom.org/wp-content/uploads/2023/07/TER-Biometrics-Humanitarian-Sector.pdf.

[14] "Practical Guidance for Data Protection in Cash and Voucher Assistance," IFRC, (January 2021), https://cash-hub.org/wp-content/uploads/sites/3/2021/01/CVA-Data-Protection-Guidance-final.pdf.

[15] Larissa Fast, "Data Sharing Between Humanitarian Organisations and Donors: Toward Understanding and Articulating Responsible Practice," Norwegian Centre for Humanitarian Studies, (June 2022), https://www.humanitarianstudies.no/wp-content/uploads/NCHS-paper-06-April-2022-Data-sharing-between-humanitarian-organisations-and-donors.pdf.

[16] Interview with responsible data expert

[17] The Centre for Humanitarian Data, "Data Responsibility in Cash and Voucher Assistance."

[18] Interview with expert on humanitarian operations

with fewer controls.[19] Sometimes data is shared raw, sometimes it is anonymised or aggregated.[20]

Snapshots of data sharing in CVA contexts

Below are some examples of CVA data sharing that came up in interviews and desk research:

- Between humanitarian organisations (pre-vetting → service delivery): According to an expert in humanitarian operations we spoke to, generally if one humanitarian organisation is pre-vetting candidates and a different organisation is responsible for service delivery, then typically the whole data package would be shared between the two organisations.[21]
- Humanitarian organisation → FSP (cash transfer): According to the same interviewee, sharing in these instances is generally restricted to recipient names, copy of ID or ID number and phone number, or whatever basic information is needed for a bank transfer to occur.[22]
- Large humanitarian organisation → national societies / local partners / FSPs (assessments + cash transfer) According to one of our interviewees with knowledge of a large humanitarian organisation's operations, data sharing can look as follows: the large organisation works with local partners and national societies (sometimes also other large humanitarian organisations) to conduct assessments, and then works with a financial service provider (e.g. bank or Telecom operator). What data is shared depends on the nature of each project. When it comes to FSPs, as a general practice the organisation only shares what is necessary for cash transfer to occur. This could include names and contact details, but it can sometimes be more aggregated than this.[23]
- Humanitarian organisation → donors (auditing): Donors might generally request aggregated data on the demographics of who is receiving CVA, and what recipients spend the money on.[24] There have been some documented cases of donors requesting more personalised programmatic data, like biometrics.[25]
- GSMA study: CVA in Somalia & Somaliland (mobile payments): The Somalia Cash working group provides CVA programming to individuals in South-Central, Puntland and Somaliland. Recipients provide data (name, phone number, photo, biometrics) to local organisations, who then provide a recipient list with Personal Identifiable Information to a larger humanitarian organisation, which sends recipient information to a Mobile Payment Service Provider (MSP) – usually via an Excel spreadsheet over email – and transfers funds to the MSP. The MSP sends the humanitarian organisation the verification status of recipients' SIM registration, then sends the funds to recipients, who will spend it at local vendors. In this example, the humanitarian organisation tracks

[19] Interview with expert on humanitarian operations

[20] Interview with privacy expert at humanitarian organisation

[21] Interview with expert on humanitarian operations

[22] Interview with expert on humanitarian operations

[23] Interview with digital security expert at humanitarian organisation

[24] IFRC, "Practical Guidance for Data Protection in Cash and Voucher Assistance," 33.

[25] Pauline Veron, "Digitalisation in humanitarian aid: opportunities and challenges in forgotten crises," ECDPM, briefing note no.143 (January 2022): 4, https://reliefweb.int/report/world/digitalisation-humanitarian-aid-opportunities-and-challenges-forgotten-crises.

transaction history through post-evaluation surveys.[26]

- GSMA study: WFP in Somalia (biometrics + mobile payments): The WFP operates slightly differently in Somalia, as they use their larger SCOPE information management and transfer platform. In this case, recipients send their name and biometrics (fingerprints) to a local partner organisation. After WFP approves eligibility recipients receive a SCOPE card, which carries their fingerprints and details. The local partner sends the recipient information as well as card details to the WFP, who transfers recipient lists and phone numbers (alongside funds) to an MSP. The MSP verifies recipient identities by matching the information to their SIM registries, and reconciles disparities with the WFP. The WFP is then able to directly transfer money to recipients via SCOPE. Recipients spend the money through approved SCOPE vendors or e-payments and the WFP is able to track transactions and purchase information.[27]

Tools and platforms currently used for data sharing

A number of major humanitarian organisations have developed their own platforms and databases for managing (and often sharing) beneficiary data; **UNHCR's PRIMES** and **WFP's SCOPE** are the two largest repositories of biometric information in the humanitarian sector. Third party tools, such as the popular data management platform **RedRose**, are also used for humanitarian data management. More details on all of these platforms can be found in the DIGID Consortium's 2023 landscape scan.[28]

One platform that surfaced in our research, UNHCR's RAIS (Refugee Assistance Information System), is worth mentioning in more detail here, as it does not appear in the landscape scan but was mentioned in several interviews as an example of a more comprehensive data sharing platform. Among other things, RAIS is used for sharing data between UNHCR and their partner organisations, for coordination purposes.[29] In these cases, access to RAIS is determined by data sharing agreements tailored to the needs of each partnership and uploaded into the system, which allows for sharing by area (such as shelter, for those who only need information related to shelter). In interviews, we were told that access to UNHCR information is determined on a case by case basis for each partner.[30]

Outside of these large central platforms, a large proportion of data sharing in the sector is conducted using more general-purpose commercial tools. Those mentioned in interviews include:

- **Excel files shared over email** (both encrypted and unencrypted).[31]
- **Spreadsheets stored and shared via cloud services.**[32] **Google Drive**[33] **and Microsoft 365**[34] were mentioned specifically.

[26] GSMA, "Developing Guidelines for Cash Transfers in Somalia," GSMA, (May 2021), https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2021/05/0_SOP-Process-Mapping_R_Web.pdf.

[27] GSMA, "Developing Guidelines for Cash Transfers in Somalia."

[28] Worthington and Duechting, "Enabling Dignified Humanitarian Assistance."

[29] "Planning and Preparing Registration and Identity Management Systems," UNHCR, accessed November 21, 2023, https://www.unhcr.org/registration-guidance/chapter3/registration-tools/.

[30] Interview with information management expert at humanitarian organisation

[31] Interview with data privacy and legal expert at humanitarian organisation

[32] Interview with digital security expert at humanitarian organisation

[33] Interview with expert on humanitarian operations

[34] Interview with data protection expert at humanitarian organisation

- Data shared through USB flash drives.[35]
- **Data shared directly with financial institutions** can often be done **directly through an Application Programming Interface (API)**.[36]

Notable data breaches in recent years

The humanitarian sector has seen a few noteworthy intrusions in recent years, but some of our interviewees estimated that many more have been going undocumented. Noting that recognising and attributing cyber attacks is very complex, one interviewee, a privacy expert and advocate said:

> "Most organisations don't have a system of monitoring when things go wrong, or people *are* finding [intrusions] and not reporting – there's so little evidence not because intrusions aren't happening, but because no-one *knows* they're happening."[37]

As a result there are limited examples of data breaches in the sector. There are, however, some that have been both noticed and documented or reported on: below we discuss a few, as well as one high-profile breach from outside the sector that is covered for its clear illustration of the potential pitfalls of relying on popular third-party software.

ICRC Restoring Family Links programme data (2021)

In late 2021, the ICRC was the target of a data breach exposing the data (names, contact details, and location) of 515,000 "highly vulnerable people." Specifically, the data that was leaked came from the Restoring Family Links programme – aimed at reuniting family members who have been separated due to natural disasters, armed conflicts and/or migration. The system's anti-malware software detected and blocked parts of the attack, but the malware largely bypassed the security measures in place. The ICRC urged the hackers to not buy, sell or share the information they obtained due to the highly sensitive nature of the data.[38]

NRC country office (2023)

In July 2023 the NRC reported that it had been targeted in a data breach that impacted a specific project in a country office. At the time of writing this report, details of the nature of the attack are still limited, including the scope of whose data was exposed. This attack appears to have targeted the personal data of project participants stored in an online database.[39]

[35] Interview with digital security expert at humanitarian organisation; interview with privacy expert and advocate

[36] Interview with data privacy and legal expert at humanitarian organisation

[37] Interview with privacy expert and advocate

[38] "Sophisticated cyber-attack targets Red Cross Red Crescent data on 500,000 people," ICRC, last updated June 19, 2022. https://www.icrc.org/en/document/sophisticated-cyber-attack-targets-red-cross-red-crescent-data-500000-people; "Cyber attack on ICRC: What we know," ICRC, last updated June 24, 2022, https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know; Jenna McLaughlin, "Cyberattack on Red Cross compromised sensitive data on over 515,000 vulnerable people," NPR, January 20, 2022, https://www.npr.org/2022/01/20/1074405423/red-cross-cyberattack.

[39] "Cyberattack on Norwegian Refugee Council online database," Norwegian Refugee Council, last updated July 18, 2023, https://www.nrc.no/news/2023/july/cyberattack-on-norwegian-refugee-council-online-database/.

Software: Blackbaud (2020) & RedRose (2017)

The breaches of Blackbaud (in 2020) & RedRose (in 2017) affected multiple humanitarian organisations using the software.

Blackbaud provides fundraising and CRM software designed to be used by non-profit organisations. A 2020 hack exposed names, addresses, and records of individual donors stored by organisations using the software – the breach affected a reported 200+ customers, including World Vision, Save the Children and Human Rights Watch.[40]

RedRose is used in the humanitarian sector for data management. In 2017, The New Humanitarian reported that an emerging competitor to RedRose had managed to access large amounts of beneficiary data due to security vulnerabilities in the system, which was being used at the time by at least 11 major humanitarian organisations, including Oxfam, CARE and Catholic Relief Services.[41]

UN networks in Geneva & Vienna (2019)

In 2020, The New Humanitarian (TNH) reported that in 2019 the UN had uncovered a cyberattack targeting its offices in Geneva and Vienna, which had compromised "dozens of UN servers – including systems at its human rights offices, as well as its human resources department … some administrator accounts [were also] breached." TNH reported that the breached servers held "a range of data, including personal information about staff." As the UN has diplomatic immunity, it has no legal obligation to report cyber attacks or data breaches to the public, and it did not do so in this case; TNH reported that even staff were not told in full about the nature of the breach, beyond being told to change and strengthen their passwords.[42]

SolarWinds (2019-2020)

While not directly targeting the humanitarian sector, the SolarWinds attack provides a high-profile and well-documented example of how far an attack can go when it targets third-party software.[43] Beginning in 2019, Russian Foreign Intelligence Service hackers breached the networks of Texas-based IT management company SolarWinds. In 2020, the hackers hid a piece of malicious code in a system update that essentially opened the door for them to gain remote access to the devices that downloaded the update. It is believed that approximately 18,000 customers (from 100 companies) received the compromised update, a smaller subset of which were targeted.[44] Eight US government agencies including the Pentagon, Treasury, Justice, DHS and Energy departments were exposed to the attack, as were government

[40] Ben Parker, "Dozens of NGOs hit by hack on US fundraising database," The New Humanitarian, August 4, 2020, https://www.thenewhumanitarian.org/news/2020/08/04/NGO-fundraising-database-hack.

[41] Nathaniel A. Raymond, Daniel P. Scarnecchia, and Stuart R. Campo, "Humanitarian data breaches: the real scandal is our collective inaction," The New Humanitarian, December 8, 2017, https://www.thenewhumanitarian.org/opinion/2017/12/08/humanitarian-data-breaches-real-scandal-our-collective-inaction; Ben Parker, "Security lapses at aid agency leave beneficiary data at risk," The New Humanitarian, November 27, 2017: https://www.thenewhumanitarian.org/investigations/2017/11/27/security-lapses-aid-agency-leave-beneficiary-data-risk.

[42] Ben Parker, "EXCLUSIVE: The cyber attack the UN tried to keep under wraps," The New Humanitarian, January 29, 2020, https://www.thenewhumanitarian.org/investigation/2020/01/29/united-nations-cyber-attack.

[43] Massimo Marelli, "The SolarWinds hack: Lessons for international humanitarian organizations," International Review of the Red Cross, no. 919 (June 2022), https://international-review.icrc.org/articles/the-solarwinds-hack-lessons-for-international-humanitarian-organizations-919.

[44] "SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (infographic)," GAO, April 22, 2021, https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic.

technology vendors like Microsoft, Intel and Cisco.[45] In 2021, Microsoft said that the same hackers behind the Solar Winds attack carried out an email phishing attack against USAID.[46]

Policies and guidance that shape data sharing

Formal agreements governing data management and sharing are key elements of risk management in humanitarian CVA, and as such are relevant to any discussion around risk mitigation. Data sharing can, however, also happen informally, especially in emergency situations.[47]

Best practices for the humanitarian sector include setting up information sharing protocols, undergoing risk assessments, establishing data sharing agreements, and making sure that these are in accordance with relevant legal constraints and obligations.[48]

Below are some of the key ways in which data is currently managed and shared in CVA.

- Data Protection Impact Assessments (DPIAs): DPIAs are the most common risk assessments conducted for CVA programmes. They typically cover the risks associated with collecting and sharing personal data but can be expanded to cover non-personal data. For organisations operating in the EU or based in the EU, GDPR standards guide the protections outlined in the DPIA. In our interviews, the tension between how DPIAs work on paper and how they operate in practice came up, as they can become a series of tick-boxes that are shaped to a project rather than considerations that might necessitate changes to the project design.[49]
- GDPR compliance: Where applicable, the GDPR offers legal guidance on the processing, retention and sharing of data. But while the GDPR details explicit cases of how and in what cases (and forms) personal data can be processed, in practice this is not always straightforward for humanitarian organisations: in emergency situations, for example, the need to provide vital services may act as a legal basis for processing personal data.[50]
- Data sharing agreements and consent forms: Data sharing agreements cover the negotiated terms and conditions guiding sharing personal data. Standards are typically set at a country level, and then the parties sharing data will sign an agreement before sharing.[51]

[45] Dina Temple-Raston, "A 'Worst Nightmare' Cyberattack: The Untold Story of the Solar Winds Hack," NPR, April 16, 2021, https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.

[46] Bill Chappell, Dina Temple-Raston, and Scott Detrow, "What We Know About The Apparent Russian Hack Exploiting a US Aid Agency," NPR, May 28, 2021, https://www.npr.org/2021/05/28/1001237516/what-we-know-about-the-apparent-russian-hack-exploiting-a-u-s-aid-agency.

[47] IFRC, "Practical Guidance."

[48] The Centre for Humanitarian Data.

[49] Interview with expert on humanitarian operations

[50] Theodora Gazi, "Data to the rescue: how humanitarian aid NGOs should collect information based on the GDPR," Journal of International Humanitarian Action 5, 9 (July 2020), https://doi.org/10.1186/s41018-020-00078-0.

[51] The Centre for Humanitarian Data, 4-5.

Section 3: Areas of potential risk & harm, and challenges to protecting data in humanitarian CVA contexts

This section looks at key elements of the CVA landscape through the lens of potential risk and harm. It's important to note here, however, that as the details of each humanitarian operation differ in any given context, so too do the associated risks. With this in mind, this section can only offer an **overview of the risk areas** that are particularly relevant to humanitarian CVA (and that came up in our research). These risks will need to be considered in specific contexts when designing any mitigation measures.

A note on scope and focus:

Many of the risk areas outlined in this section apply to humanitarian data collection and sharing in general, and not just to CVA operations – these are included as they will be important to consider in any effort to mitigate risks related to data sharing in CVA.

It should also be noted that risks, when realised, can often have impacts for both the people whose data has been collected and processed, and for humanitarian organisations themselves (for example, reputation damage and loss of trust); the magnitude of harm, however, generally falls disproportionately on the data subjects, and this is the focus of this report.

To evaluate risk, it is crucial to properly consider potential harms

In our research, while there is increasingly robust discussion around the risks involved in humanitarian collection and sharing of data, **we encountered less discussion around potential harms to the subjects of that data** – i.e. the people whose data is processed by humanitarian organisations.

Linking harms to specific instances of humanitarian data collection can be challenging

The relative lack of discussion around harms compared to that around risk may in part be due to the fact that the initial act of data collection and instances of actual harm can be difficult to connect. Harms caused by illegitimate use of data collected in a crisis situation can occur in a **very different time and place** to the original context – as a result, it can be difficult for humanitarian organisations to determine with certainty, or anticipate the full scope of, potential harm that may be associated with data that they have collected, stored and shared.

One interviewee sketched out the following scenario by way of example: "People move on, and end up, for example, seeking asylum somewhere else – there could be something [in data that the potential host government has access to] that means they get rejected. The data was collected years before by a humanitarian organisation, and then stored and shared, but you might not be able to trace it back to that moment."[52]

In humanitarian discussions, **biometrics have been most clearly linked to potential long-term harms** – many interviewees we talked to noted the sensitive nature of biometric information and the immutability of biological features recorded. To date there have already been documented cases of biometric data collected to facilitate humanitarian assistance **landing up in hostile hands**: in the humanitarian sector, the most well-known example is from Bangladesh, where Rohingya data was shared with the government they had fled from, Myanmar – according to a Human Rights Watch investigation, very likely without their informed consent.[53]

Both 'sensitive' and 'non-sensitive' (including operational) data can be used to facilitate harm

Discussion of harms in the context of humanitarian data collection tends to focus specifically on sensitive data (such as political affiliation, current location, ethnicity and sexuality) being used for unintended purposes.[54] It is, however, very possible for non-sensitive data to be combined with other data sets to reveal sensitive information, or to re-identify individuals from 'anonymised' lists. (More on this can be found later in this section)

Harms can also be facilitated by **operational, non-personal data**. This type of data can be less protected than more obviously sensitive data, but there are in fact concrete harms that can result from this data landing up in hostile hands: for example, the precise location of infrastructure such as medical facilities, educational facilities, computer servers and so on may place individuals in those locations, or dependant on those facilities, at risk of harms such as targeted violence, disruption of services, and unauthorised access to sensitive data.[55]

[52] Interview with privacy expert and advocate

[53] Irwin Loy, "'It's like the wild west': Data security in frontline aid," The New Humanitarian, February 28, 2022, https://www.thenewhumanitarian.org/interview/2022/02/28/data-security-in-frontline-aid.

[54] IFRC, "Practical Guidance."

Harms can include financial repercussions, discrimination and stigma, and physical violence

In our interviews, a number of concrete examples surfaced of people who were receiving assistance, or who had received assistance in the past, appearing on **watch lists**, or being subject to **violence, stigmatisation, and discrimination.**[56] The following cases surfaced in our research:

- **Financial repercussions.** This type of harm was especially emphasised in our interviews – merely being identified as a person who has received aid in the past can be enough to be denied a bank loan, for example. One interviewee gave the following example of a case they had observed: "an individual who was given assistance during conflict meant they were denied a loan in a post-conflict setting – [the fact of receiving assistance] made them not seen as creditworthy; the bank was worried they'd fall back into a situation of vulnerability."[57]
- **Stigmatisation and discrimination.** This too can result from merely being identified as having received assistance. A concrete example was given in interviews of children being stigmatised at school because of this.[58]
- **Violence enabled by location tracking.** In active conflict zones, location data and location history can allow hostile actors to trace individuals or even group movement, and find "safe spaces" that groups may have moved to. This can also happen after a conflict has ended.[59] Where recipients of assistance are refugees in host communities where some members are hostile towards them, location data can direct these hostile members to their whereabouts.[60] Location data can also enable hostile governments to track them.[61]
- **Violence facilitated by leaked data on ethnicity or political affiliation.** In ethnic or political clashes, leaked data can furnish hostile actors with the information they need to target specific groups and individuals.[62]

Sharing data almost inevitably adds an extra degree of risk

When looking at data sharing in the humanitarian sector, it is important to note that the sharing of data – however this is done technically, and whether data is copied or not – is almost always accompanied by a degree of risk.[63] This is because:

[55] OCHA, "Data Responsibility Guidelines," OCHA Centre for Humanitarian Data, (October 2021), https://data.humdata.org/dataset/2048a947-5714-4220-905b-e662cbcd14c8/resource/60050608-0095-4c11-86cd-0a1fc5c29fd9/download/ocha-data-responsibility-guidelines_2021.pdf.

[56] Interview with privacy expert and advocate

[57] Interview with privacy expert and advocate

[58] Interview with responsible data expert

[59] Jill Capotosto, "The mosaic effect: the revelation risks of combining humanitarian and social protection data," Humanitarian Law and Policy, February 9, 2021, https://blogs.icrc.org/law-and-policy/2021/02/09/mosaic-effect-revelation-risks/.

[60] Interview with data privacy and legal expert at humanitarian organisation

[61] Linda Raftree, "Responsible Data Sharing with Governments," CALP Network, (March 2021): 4, https://www.calpnetwork.org/wp-content/uploads/2021/03/CaLP-Case-Study-Responsible-Data-Sharing-with-Governments.pdf.

[62] Veron, "Digitalisation in humanitarian aid."

[63] Jo Burton, ""Doing no harm" in the digital age: What the digitalization of cash means for humanitarian action," International Review of the Red Cross, no. 913 (March 2021), https://international-review.icrc.org/articles/doing-no-harm-digitalization-of-cash-humanitarian-action-913.

- Each time data is shared, the 'surface area' of risk gets bigger. The more people who have access to data (whether or not the data is in their possession) – the more chances there are for other parties to gain access to it. As one interviewee, a responsible data expert, said: "The more people who have data, the more exposure there is – even if there are no threats from threat actors, there's still human error. Even well-resourced, highly secure systems are vulnerable. There's a real risk of exposure, and data sharing increases the exposure surface; this includes more people having access."[64]
- Sharing inevitably involves a loss of control. Once data is shared, the organisation that originally collected and shared it can't truly know where the "end point" is. This is something that can never be fully mitigated through data sharing agreements.
- Sharing can complicate or invalidate consent. Sharing data can make consent from people receiving assistance difficult to navigate. While systems like RAIS (mentioned in Section 2) are useful in creating tailored data sharing arrangements, when access is negotiated on a case by case basis it can be complicated to accurately communicate the myriad of ways data subjects will have their data used, shared and stored. This is especially nuanced in situations where people give their consent very early on (e.g. refugee registration data) prior to considering factors like CVA or shelter logistics, for instance.[65]

Alongside all this is the unfortunate fact that efforts to "anonymise" data may not be sufficient to prevent leaking sensitive information about the individuals in the original dataset. More on this can be found later in this section.

General ways in which data can be compromised

Aside from those who have direct access to data, there are a number of ways in which third parties can gain unauthorised access to a system or to data, and these are generally well known and documented. This report does not aim to provide an exhaustive discussion of general security threats; however, any initiative that aims to address data security should keep the following in mind.

Common ways in which stored data can be compromised

- Phishing — this is a common method used to steal certain types of access credentials, and can target any individual in the supply chain.
- Spyware — can allow access to both credentials and data through compromised devices. State-sponsored, targeted spyware in particular – which can allow persistent access to both credentials and data through compromised devices – is very difficult to both prevent and detect.[66]
- Direct attacks — hostile actors might target data management infrastructure directly.
- Legal requests — if data is stored in a location that falls under the relevant jurisdiction, law enforcement or government can legally require access to it. This is important to

[64] Interview with responsible data expert

[65] Read more on consent in CVA operations: IFRC, "Practical Guidance;" Christopher Kuner and Massimo Marelli, co-eds., "Handbook on Data Protection in Humanitarian Action," ICRC, (June 2022), https://www.icrc.org/en/data-protection-humanitarian-action-handbook; Amos Doornbos, "Consent and Ownership in the Shift to Digital Cash and Voucher Assistance," CALP Network, November 11, 2019, https://www.calpnetwork.org/blog/consent-and-ownership-in-the-shift-to-digital-cash-and-voucher-assistance/.

[66] Steven Feldstein and Brian (Chun Hey) Kot, "Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses," Carnegie Endowment for International Peace, (March 2023), https://carnegieendowment.org/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses-pub-89229.

note when it comes to third party software and cloud services.

It should also be noted that the more data is available in one location (for example, a centralised database), the more attractive that location can become as a target.

Ways in which data can be read in transit

When data is transferred between organisations, there is the risk that it can be accessed by outside parties along the way.

- When sending data via **unencrypted email,** for example, each email server on the path between sender and receiver can access the data.
- Similarly, when **transferring or sharing a file** via a third party service provider that has not set up their systems to use end-to-end encryption (E2EE – see more on this in the Annex) — as is the case with, for example, commonly-used services like WeTransfer or Mega, Microsoft OneDrive/Sharepoint or Google Cloud or Dropbox, the provider can usually access the file.
- **Attacking the network infrastructure** is more challenging, but not impossible – a successful attack would, however, need to involve the ability to both access the traffic (for example, via a re-routing attack or DNS poisoning), *and* the ability to decrypt it (for example, through a person/machine-in-the-middle attack, by compromising Certificate authorities,[67] and so on).

Each stakeholder in a CVA data flow is a potential source of risk

When assessing risk, each stakeholder in a CVA data flow is a node that should be considered as a point of vulnerability for outside parties to potentially gain access to information.

Different stakeholders are also likely to have different understandings of protection and compliance, different appetites for risk, as well as varying levels of ability to navigate different legal regulations, provide data protection measures, and train staff, among other factors. Any additional access points within a data sharing ecosystem can have a multiplier effect on risk.

Below is a list of key stakeholders to take into account in any risk analysis, with some of the key ways in which each stakeholder might contribute to increased risk.

Humanitarian organisations' operational complexity can add risk

Humanitarian organisations are the primary collectors of data when it comes to CVA programming.

A clustered approach to humanitarian service delivery results in more organisations operating in the same context, which can lead to datasets being replicated across organisations or shared between them.

Humanitarian organisations' decentralised operational models can also make it challenging for them to ensure policies are being properly implemented.

[67] Dan Goodin, "State-Sponsored Hackers in China Compromise Certificate Authority", Ars Technica, November 15, 2022, https://arstechnica.com/information-technology/2022/11/state-sponsored-hackers-in-china-compromise-certificate-authority/.

Third party software & infrastructure providers, financial service providers, and monitors and auditors can all add risk in multiple ways

As more private sector actors provide services to the humanitarian sector, their involvement can increase the risk profile of data sharing.

The humanitarian sector's use of external commercial software and cloud computing in particular – such as the establishment of a Microsoft office inside the UN and the integration of MS365 in UN agencies[68] – has created a reliance on private sector organisations that have developed solutions initially for commercial purposes that are then reused in humanitarian contexts.

And while some humanitarian organisations do use purpose-built central registries, these are sometimes deployed by third party providers (for example, RedRose).

Humanitarian data is also **regularly shared with third-party monitors** that report to donors, but, as the Global Public Policy Institute reports, those sharing the data tend to "know little about how these entities process the data, whether it is immediately destroyed after use, or whether it may be shared with third parties such as host governments or commercial companies."[69]

When it comes to CVA in particular, third party providers (including banks) are also often used to provide **financial services**, as well as monitoring and auditing services.

There are a number of ways in which third parties can add increased risk:

- Access to data:
  - Third party **software providers** often have potential access to **data & metadata** that is stored on, or that passes through, their platforms. Even when data is stored encrypted on a third-party platform, the provider often holds the **decryption keys**. Third-party providers also generally have access to the **(unencrypted) metadata** that is created by the people who use their services.[70] As a digital security expert at a humanitarian organisation explained, "All the data that's being shared that organisations may not realise is being shared – this is different to the 'declared' data; it's the hidden side – the data that is generated as you use these services."[71]
  - **Financial Service Providers (FSPs)** generally collect **transaction data**, which can reveal both individual and community-level decision-making patterns (more on this can be found later in this section). While this information is captured legitimately, it is done so often without the knowledge of the individuals involved.
- **Conflicting interests:** The humanitarian sector has been criticised in the past for its collaborations with private sector software providers – of particular concern is that the private sector's interests, incentives and standards can run counter to humanitarian principles and standards, and this could compromise humanitarian work. [72] [73]

[68] "Why does Microsoft have an office at the UN? A Q&A with the company's UN lead," Microsoft, October 5, 2020, https://news.microsoft.com/on-the-issues/2020/10/05/un-affairs-lead-john-frank-unga/.

[69] Florian Westphal and Claudia Meier, "Research on the Specific Risks or Constraints Associated with Data Sharing with Donors for Reporting Purposes in Humanitarian Operations," GPPI, (August 2020), https://www.gppi.net/media/GPPi_DonorDataSharingRisks_Report_August2021.pdf.

[70] International Committee of the Red Cross (ICRC) and Privacy International, "The Humanitarian Metadata Problem: "Doing No Harm" in the Digital Era," Privacy International, (October 2018), https://privacyinternational.org/sites/default/files/2018-12/The%20Humanitarian%20Metadata%20Problem%20-%20Doing%20No%20Harm%20in%20the%20Digital%20Era.pdf.

[71] Interview with privacy expert and advocate

[72] "One of the UN's largest aid programmes just signed a deal with the CIA-backed data monolith Palantir," Privacy International, February 12, 2019, https://privacyinternational.org/news-analysis/2712/one-uns-largest-aid-programmes-just-signed-deal-cia-backed-data-monolith.

- **Differing legal obligations and relationships:** Private sector organisations may have different legal obligations or relationships with other parties, such as governments or other external actors. This can result in them being more willing, or less able to refuse, to share data – potentially also without disclosing that data has been shared.[74] This is particularly relevant when it comes to **humanitarian agencies with immunities** (such as the UN and ICRC), as these privileges are generally not shared by third-party partners. **Financial service institutions** specifically (e.g. banks and other providers of financial services such as internet and telecom service providers or mobile payment solutions) may be asked to share data with regulators; some might also be affiliated with the government.
- **Third party platforms can be appealing targets:** While security can be cited as a reason to use popular third party products, a breach of a widely-used system can have equally wide impacts. The large number of organisations using SolarWinds software, for example (see Section 2), meant that those who attacked that software were able to have a huge impact. This potential can make these kinds of platforms appealing targets.

Donor requests and requirements can drive over-collection

As a key stakeholder in CVA, donors have a great deal of power in shaping what type of data is collected, where it is stored and how it is shared, and they are often drivers and instigators of data collection for monitoring & auditing (potentially via third party auditors) and impact measurement, typically for transparency in their humanitarian spending.[75]

In some cases, just the possibility that data may be requested can lead to **pre-emptive over-collection** that is often contrary to data minimisation efforts[76] – a "collect as much as we can mentality", as one interviewee described it.[77] This is fuelled in part by what another interviewee described as a fear that "if they don't gather the data [now], they won't have it when they need it later; for example, for follow-up." [78]

Donors have in some cases **requested** that data be stored in specific databases, such as WFP's SCOPE, or UNHCR's PRIMES (for example, where an implementing partner is working in partnership with these organisations). At times these requests may also stipulate that certain forms of data, such as biometrics, be collected (which can pose increased risks), or that data sharing between organisations take place.[79]

There is currently controversy over such requirements, and concern over talks to make some humanitarian databases interoperable with government institutions as well.[80] The data requested by donors is meant to take the form of aggregated data, but instances of informal requests for individual-level data have been reported.[81]

[73] Nathaniel Raymond, Laura Walker McDonald, and Rahul Chandran, "Opinion: The WFP and Palantir controversy should be a wake-up call for humanitarian community," Devex, February 14, 2019, https://www.devex.com/news/opinion-the-wfp-and-palantir-controversy-should-be-a-wake-up-call-for-humanitarian-community-94307.

[74] Interview with privacy expert and advocate

[75] Raftree, "Data Responsibility Toolkit."

[76] Fast, "Data Sharing Between Humanitarian Organisations and Donors," 14.

[77] Interview with privacy expert and advocate

[78] Interview with expert on humanitarian operations

[79] Veron, 4.

[80] Raftree.

[81] Fast, 12.

Governments have a variety of incentives to gain access to data collected by humanitarian organisations

Hostile governments (along with other local groups) in areas of ongoing conflict may have an incentive to gain access to beneficiary data, in order to inflict violence or engage in discriminatory practices on certain groups of individuals, or to control their movements. In some cases, they may be able to obtain data held by humanitarian organisations through **legal means**.

Governments hosting humanitarian activities (host governments) may request CVA data within their jurisdictions to monitor these activities and/or resolve any disputes over social protection.[82] Host governments may also seek information on individuals to **restrict movements, monitor access to support, or surveil refugees** for adherence to employment or other constraints.[83]

Host governments can in turn **hand over data to other governments** – as was the case when Bangladesh shared data about Rohingya refugees with the government of Myanmar.[84] Across the sector, there is evidence of some belief (to varying degrees) that host governments have a legitimate interest in knowing who is on their territory.[85] Consequently, data might be given over by actors in the CVA ecosystem even if not legally mandated.

Discussions around integrating CVA and social protection: what this might mean from a data sharing and risk perspective

Recently, discussions in the sector around integrating humanitarian assistance with social protection administered by governments have gained traction due to the potential for longer term impact and greater service reach.[86] CVA in particular is seen as a natural converging point between humanitarian work and social protection programmes. In the Philippines, for example, WFP and UNICEF helped top up social payments coming from the department of social welfare, and in Mauritania the Finance ministry is in a cash consortium with NGOs.[87]

Linking CVA programming to ongoing social protection programmes would, however, require increased data sharing with governments, potentially through shared databases.[88] With social protection likely to become a bigger part of CVA programming, it is important to pay close attention to the ways in which governments may raise the risk profile of data sharing, and ensure that any data collection and sharing protocols are designed with these possibilities in mind.

Other governments not involved, or only peripherally involved, in the immediate context may seek humanitarian data for migration purposes. (The US government, for example, seeks access

[82] IFRC, 29-30.

[83] Raftree, ""Responsible Data Sharing with Governments."

[84] "UN Shared Rohingya Data Without Informed Consent," HRW, June 15, 2021, https://www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent.

[85] Interview with privacy expert and advocate

[86] Daniel Longhurst, Paul Harvey, Rachel Sabates-Wheeler, and Rachel Slater,"Linking Social Protection and Humanitarian Cash and Voucher Assistance," CALP Network, (April 2020), https://www.humanitarianoutcomes.org/sites/default/files/publications/high-level-briefing-paper-cva-en.pdf.

[87] Ugo Gentilini, Sarah Laughton, and Clare O'Brien, "Human(itarian) Capital? Lessons on Better Connecting Humanitarian Assistance and Social Protection," World Bank Group, discussion paper no. 1802 (November 2018), https://documents1.worldbank.org/curated/en/946401542689917993/pdf/Human-itarian-Capital-Lessons-on-Better-Connecting-Humanitarian-Assistance-and-Social-Protection.pdf.

[88] Edward Archibald, "Mapping and Analysis of Social Protection in Sudan," South Sudan Ministry of Gender, Child and Social Welfare and the United Nations Children's Fund (UNICEF), (July 2019), https://www.unicef.org/southsudan/media/3251/file/South%20Sudan%20National%20Social%20Protection%20Mapping.pdf.

to biometric data as part of resettlement applications for counter-terrorism purposes.) These governments may have varying degrees of power and ability to request and obtain data; they might also be targets of attack themselves, as was the case in 2022 with the breach of a US Immigration and Customs (ICE) database that exposed the personal data (names, birthdates, nationality and detention centres) of over 6,000 migrants, including those fleeing persecution and torture.[89]

Hostile non-government actors might seek out data for tracking and targeting

Hostile non-governmental actors interested in violence or retribution may also seek out humanitarian data on refugees or people on the move.

In Yemen, for example, the Houthi leadership objected to the WFP's rollout of SCOPE in Houthi-controlled Sana'a.[90] Fearing that the SCOPE system would limit Houthi supervision, Houthi leadership argued that the biometrics system should be run by the Yemeni Social Welfare fund – a Sana'a based organisation.[91] The WFP partially suspended aid before agreeing to a joint server housed in Yemen.[92]

Tensions over the control of data collection processes in Yemen illustrate how data can be politicised during conflict, and how non-government actors might have specific interest in data within a conflict environment.

Specific challenges that the CVA ecosystem presents for data security

Any use of technology to collect, store and share data comes with its share of risk, and humanitarian systems appear to be increasingly becoming targets. When looking specifically at risk in humanitarian CVA, it's important to look at the entire "supply chain" of any system, as intrusions can, and frequently do, target perceived weak points in the chain (for example, as already mentioned, a third-party software provider, or an employee at a partner organisation).[93]

CVA programming involves pressure to collect more extensive information

In CVA programming particularly, organisations have greater pressure and tendency to collect extensive information, especially sensitive information such as biometrics as part of Know Your Customer requirements and compliance measures for counter terrorism and Anti Money Laundering regulations.[94] The nature and extent of data collection, as well as the expectations of data sharing, increase the risks associated with data sharing in CVA operations.

[89] Hamed Aleaziz, "ICE accidentally released the identities of 6,252 immigrants who sought protection in the U.S.," LA TIMES, November 30, 2022, https://www.latimes.com/california/story/2022-11-30/ice-released-names-6252-immigrants-persecution.

[90] Marie-Loiuse Clausen, "Piloting Humanitarian Biometrics in Yemen," PRIO Middle East Centre, (2021), https://mideast.prio.org/utility/DownloadFile.ashx?id=65&type=publicationfle.

[91] Aziz El Yaakoubi and Lisa Barrington, "Yemen's Houthis and WFP dispute aid control as millions starve," Reuters, last updated June 4, 2019,https://www.reuters.com/article/us-yemen-security-wfp-idUSKCN1T51YO.

[92] World Food Programme, "Internal Audit of WFP Operations in Yemen," Office of the Inspector General/Office of Internal Audit, (January 2020), https://docs.wfp.org/api/documents/WFP-0000113105/download/.

[93] Marelli, "The SolarWinds hack."

[94] Raftree, "Data Responsibility Toolkit."

Keeping technical systems properly maintained requires a level of resources that most organisations don't have

As organisations begin to lean on technical solutions to manage risk, **more time and resources are required to maintain them**, and the more possibility there is that issues may arise from a lack of maintenance or expertise.

Relatively small budgets and a general lack of cybersecurity experts and requirements within organisations mean that even when well-meaning data sharing policies are in place, data can still be vulnerable to being compromised, [95] and technical systems are often not monitored to the degree that they could be. One interviewee, a digital security expert at a humanitarian organisation, suggested outsourcing as a possible alternative:

> "It's unusual that these organisations have highly skilled teams with lots of capacity, like a security operations centre. Or they outsource it [security monitoring] to a third party, who will, for example, look at the screen or auto-raised flags and then investigate."[96]

However, outsourcing to third parties brings other risks, as discussed earlier in this report.

The need to respond adequately to individual contexts can be in tension with protocols

Adapting operations to different contexts is necessary, but is also likely to result in **different systems and processes** being used to store, share and protect data. As one interviewee told us: "There's a tension between the current drive for localisation and so on, and the importance of data security – when you have a proliferation of systems, it's hard to have standards." [97]

One interviewee – a digital security expert at a large humanitarian organisation – said that in any data sharing agreement or system it's important to take into account the realities of the field:

> "Sometimes you just need to share something with a colleague – we try to avoid email but USB sticks can be used if you do certain things – for example, if you know where [the USB stick] comes from, and encrypt the things on it. There is space for agreeing – again, depending on the level of risk – … we don't want to say "whatever you do, use this".[98]

Rapid changes in contexts can leave technical infrastructure (and the data it stores) vulnerable

Humanitarian organisations operate across a range of contexts, with differing considerations and pressures. Crucially, these contexts are often dynamic and can shift quickly.[99]

If an organisation needs to move out of an area rapidly, for example, systems left behind may be in jeopardy. In this type of situation, potential mitigation measures can pose their own risks: one interviewee noted that functionalities such as remote commands to wipe computers, for example, could leave humanitarian workers vulnerable.[100]

[95] Interview with digital security expert at humanitarian organisation

[96] Interview with digital security expert at humanitarian organisation

[97] Interview with responsible data expert

[98] Interview with digital security expert at humanitarian organisation

[99] Interview with data protection expert at humanitarian organisation

[100] Interview with data protection expert at humanitarian organisation

Systems holding biometric data left behind in Afghanistan

When the Taliban took over Afghanistan they gained access to personal information collected by foreign governments and international institutions on Afghans who had assisted American troops as translators and in other support roles, raising fears that these Afghans or their families may be targeted.[101]

The instability of humanitarian crises mean that organisations may need to leave swiftly. And as one interviewee asked: “When something goes bad, how can you stop the data being useful [to malicious actors]?”[102] Even just by attesting to particular interactions between individuals, humanitarian records can be weaponised.

Data protection policies can be implemented in uneven and uncertain ways

Policies are used in the humanitarian sector as a **key element of data protection** and risk management.

However, **reliance on policy** to ensure data is correctly collected, shared and stored can be misplaced in the complex humanitarian operational environment. Though data sharing agreements and data protection policies set out how sharing is meant to take place, humanitarian organisations often have limited ability to ensure policies are being properly followed and enforced, which can result in policies being **misunderstood, overlooked or ignored.**

As one interviewee, a data protection expert at a humanitarian organisation, said: “you can have a policy that says you should do a DPIA – but people can ignore it.”[103]

There are a number of factors that contribute to this:

- **Lack of skill or understanding needed to properly implement policies.** As a digital security expert at a humanitarian organisation we spoke to said: “You can sign a contract, consent forms, write a policy – but at the end of the day that won't prevent someone from doing something wrong. Reality sometimes bites.”[104]
- **Lack of the time and resources needed to properly implement policies**. Especially in cases where policies are complex, or perceived to add to workloads, humanitarian workers can often resort to more efficient – but less secure – informal workarounds, such as sending excel sheets via email. As a privacy expert and advocate told us, in practice it can be very difficult to do things “by the book”.[105] Another observed: “Very few people end up looking at contracts and agreements afterwards. So while there might be all these things in place, there can be very little enforcement; there isn't the necessary follow-up. The organisation moves on to the next agreement, the next contract – and the existing ones fall through the cracks.”[106]

[101] Eileen Guo and Hikmat Noori, “This is the real story of the Afghan biometric databases abandoned to the Taliban,” MIT Technology Review, (August 2021), https://www.hrw.org/news/2022/03/30/new-evidence-biometric-data-systems-imperil-afghans; https://www.technologyreview.com/2021/08/30/1033941/afghanistan-biometric-databases-us-military-40-data-points/.

[102] Interview with digital security expert at humanitarian organisation

[103] Interview with data protection expert at humanitarian organisation

[104] Interview with digital security expert at humanitarian organisation

[105] Interview with digital security expert at humanitarian organisation

[106] Interview with privacy expert and advocate

- Lack of baseline knowledge around data protection principles & minimum standards, and around the importance of good data protection practices. Issues related to this lack of baseline knowledge were noted across the majority of our interviews. This can result in bad practices, as well as variation in how policies can be interpreted (the potential subtleties and nuances of 'necessary interest' under GDPR, for instance, may result in data being shared in ways that were not foreseen by the people who created the policy).
- Lack of ability to audit third parties for compliance. For humanitarian organisations to be certain their policies are being properly implemented, they need to ensure that third parties – states, financial institutions and other service providers – are in compliance.[107] A thorough audit of a third party's practices is, however, not always possible due to the high level of access, oversight and resources that can be required to be sure of adherence.

While standards and shared expectations are an important aspect of data management and protection, these extensive restraints mean that humanitarian organisations can't rely solely on policies to ensure data (including shared data) is handled safely and correctly.

A number of those we spoke to also questioned how possible it is to have higher-level discussions about data protection and data-sharing policy in the face of more fundamental challenges to being able to protect data effectively.

Legal data protection frameworks vary widely, and are not enough to ensure protection

Jurisdictional processes (whether international or national) vary, and broadly are insufficient to ensure the protection of data. This is especially true of sensitive data such as biometrics, which is generally absent from legal frameworks.[108]

- A lack of coherent regulation risks data being processed and shared in inconsistent or conflicting ways, or incorrectly and in ways that could lead to harms, due to misunderstanding or confusion.
- Different models of governance can apply to different parties in the data ecosystem. As has already been discussed, humanitarian organisations and third parties such as states, financial institutions and other service providers can be subject to different models of governance – which can be especially relevant to humanitarian organisations afforded immunities and privileges, such as the UN and ICRC, as these immunities and privileges generally do not extend to third parties.
- Wider human rights based legal frameworks, with their emphasis on the individual, are limited in the protections they can provide.[109]
- Legal standards of data protection can clash between jurisdictions, which can create legal risk for partners or local entities.[110] Humanitarian organisations who qualify for immunity from legal requirements (such as the UN and ICRC) can also in some cases have two-tiered agreements – one for sharing data with other organisations that have

[107] Interview with privacy expert at humanitarian organisation

[108] Mirca Madianou, "The Biometric Assemblage: Surveillance, Experimentation, Profit, and the Measuring of Refugee Bodies," Television & New Media, 20 (July 2019): 581-599, https://doi.org/10.1177/1527476419857682;

Sacha Robehmed, "The future of biometrics: Digital ID and Lebanon," SMEX, (January 2021), https://smex.org/wp-content/uploads/2021/01/210121_SMEX_PI_ElectoralDigitalID_Draft5_EN.pdf.

[109] Andrej Zwitter and Oskar Josef Gstrein, "Big Data, Privacy and COVID-19 – Learning from Humanitarian Expertise in Data Protection," Int J Humanitarian Action 5, 4 (2020), https://doi.org/10.1186/s41018-020-00072-6.

[110] CALP, "Registration, Targeting and Deduplication: Emergency Response inside Ukraine Thematic paper," CALP Network, (September 2022), https://www.calpnetwork.org/publication/registration-targeting-and-deduplication-emergency-response-inside-ukraine-thematic-paper/.

their own immunity, and one for sharing with organisations that don't have immunity, such as local NGOs. Sharing data with organisations that have immunity can create complexity in the data sharing environment, and open up potential risk for organisations with immunities.

- Loopholes or insufficiently thorough legislation may allow governments to leverage national legislation to gain access to information or assert their right to information.[111] This may nullify the conditions of data sharing agreements.

Some legal regulations require data collection and sharing in CVA, and some restrict it

Data collection and sharing can in some cases be required in order to comply with specific legal rules and regulations. Depending on the specific legal frameworks that are applicable in any situation, laws can either add risk or potentially reduce it. Jurisdictions to take into account include not just the countries in which the humanitarian work is being conducted and the countries in which humanitarian organisations and their partners are based, but also the countries in which third party providers are based (including software and hosting providers), and where servers storing data are located.

Laws that can require collection and sharing of CVA data include:

- AML (Anti-Money Laundering) regulations, which include KYC (Know Your Customer) laws.
- Counter-terrorism regulations
- Local laws that humanitarian organisations might be subject to.
- Key legal frameworks that enforce limits to data collection or sharing, or allow for organisations to refuse to collect and share data, include::
- The GDPR: Humanitarian organisations established in the EU or working with those based in the EU must abide by GDPR standards for processing personal data, which includes guidance on data minimisation and purpose limitation.[112]
- Immunities: UN bodies have immunity from legal processes and are not bound to the same standards as other humanitarian organisations are.[113]

CVA and Know Your Customer (KYC) regulations

Some humanitarian organisations and financial institutions must collect due-diligence data on bank customers/recipients of money as part of **anti-money laundering and terrorist financing measures**.

- This **typically takes the form of ID checks** (as well as other documentation checks like proof of address, phone numbers and occasionally biometrics) for new bank accounts

[111] Barnaby Willitts-King and Alexandra Spencer, "Responsible data-sharing with donors," Humanitarian Policy Group, (December 2020), https://cdn.odi.org/media/documents/Responsible_data-sharing_with_donors_accountability_transparency_and_data_prot_q6t86wF.pdf.

[112] Gazi, "Data to the rescue."

[113] "Convention on the Privileges and Immunities of the United Nations," UNICEF, accessed November 21, 2023, https://www.unicef.org/auditandinvestigation/media/1421/file/Convention%20on%20UN%20Privileges%20and%20Immunities.pdf.

and customers.[114] Periodic re-verifications might be required over time.[115]

- These regulations **vary by country standards**, with some including additional measures of running names against watchlists or police databases.

The IFRC has published guidance on choosing a financial service provider (FSP) for CVA, taking into account KYC regulations.[116]

Aggregated, 'anonymised' and other 'non-personal' data can nonetheless reveal sensitive information in humanitarian contexts

Discussions around data and risk tend to separate sensitive and non-sensitive data into different tiers of risk – a division that overlaps with assessments of personal versus non-personal data collected by agencies.

In humanitarian settings, however, non-personal, aggregated or "anonymised" data can become sensitive (and as such, pose elevated risks) due to either the larger context or because of techniques used to de-anonymise datasets. This is known as **de-anonymisation** or **re-identification,[117] [118] which can be described as** "a process by which de-identified (anonymised) data becomes re-identifiable again and thus can be traced back or linked to an individual(s) or group(s) of individuals through reasonably available means at the time of data re-identification."[119]

Of particular concern is a technique known as **mosaicking,**[120] which is the process of combining overlapping datasets to reveal new information, or to identify groups or individuals. This is made easier the more details and characteristics about people that are recorded.

Datasets can also be combined with patterns inferred from metadata, including **transaction data,** which is often collected in CVA, and which can include **timestamps and location data. Transaction data** can be used not just to re-identify individuals from "anonymised" datasets, but also to infer information such as religious affiliation and political views,[121] decision-making patterns and habits, and location.[122]

This means that when considering risk, all types of data need to be included as potential sources of risk to individuals.

Some have expressed concern about this issue: In an assessment of an accelerated cash-transfer pilot in Vanuatu, for example, Oxfam expressed concerns around "issues of privacy,

[114] Electronic Cash Transfer Learning Action Network (ELAN), "ELAN Humanitarian KYC Case Studies," CALP Network, (2017), https://www.calpnetwork.org/publication/elan-humanitarian-kyc-case-studies/.

[115] Kennedy Kipkemboi, Jim Woodsome, and Michael Pisa, "Overcoming the Know Your Customer hurdle: Innovative solutions for the mobile money sector," GSMA and Center for Global Development, (2019): 6, https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/Overcoming-the-KYC-hurdle-Innovative-solutions-for-the-mobile-money-sector-1.pdf.

[116] IFRC, 24-25.

[117] Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," UCLA Law Review, (August 2010), https://www.uclalawreview.org/pdf/57-6-3.pdf.

[118] Arvind Narayanan and Vitaly Shmatikov, "Robust De-anonymization of Large Sparse Datasets," The University of Texas Austin, (2008), https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf.

[119] OCHA, "Data Responsibility Guidelines."

[120] Stephanie Diepeveen, John Bryant, Farhia Mohamud, Mahad Wasuge, and Hassan Guled, "Data Sharing and Third Party Monitoring in Humanitarian Response," HPG Working Paper, (2022), https://cdn.odi.org/media/documents/HPG_WP_Data_sharing_final_Ghe2Auu.pdf.

[121] Capotosto, "The mosaic effect."

[122] Burton, ""Doing no harm" in the digital age."

power, and potential risk of **pseudonymous transaction records** available in real-time or near real-time."[123]

A note on specific anonymisation techniques

K-anonymity is a common data anonymization and data publishing technique[124] that aims to limit the leakage of anonymized datasets – however, research has shown that sensitive data can nevertheless be inferred.[125] More recent techniques use machine learning to create a synthetic version of the original dataset while still capturing its key characteristics, but the way these models are created can still leak information about the original dataset.[126]

For a discussion about potential approaches to mitigating some of the risks discussed in this section, see the Annex.

[123] Björn Rust, "Unblocked Cash: Piloting Accelerated Cash Transfer Delivery in Vanuatu," Oxfam, (October 2019): 50, https://policy-practice.oxfam.org/resources/unblocked-cash-piloting-accelerated-cash-transfer-delivery-in-vanuatu-620926/.

[124] Latanya Sweenie,"k-Anonymity: A Model for Protecting Privacy," International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10, 5 (2002), https://dataprivacylab.org/dataprivacy/projects/kanonymity/kanonymity.pdf.

[125] Ashwin Machanavajjhala, Johannes Gehrke, Daniel Kifer, and Muthuramakrishnan Venkitasubramaniam, "ℓ-Diversity: Privacy Beyond k-Anonymity," 22nd International Conference on Data Engineering (ICDE'06), (2006), https://personal.utdallas.edu/~muratk/courses/privacy08f_files/ldiversity.pdf.

[126] Theresa Stadler, Bristena Oprisanu, and Carmela Troncoso, "Synthetic Data – Anonymisation Groundhog Day," USENIX, (2022), https://www.usenix.org/system/files/sec22summer_stadler.pdf.

Conclusion

Ensuring safe data sharing is challenging at the best of times, but even more so in resource-restricted, high-pressure environments like those humanitarians work within.

The sheer extent of the risks, threats and considerations covered in this report is indicative of how challenging it can be to thoroughly protect data. This does not mean that data should never be shared in humanitarian work, including CVA – but it does encourage an intentional and limited approach to data sharing, which should extend to any technical systems designed to facilitate this.

Ultimately, even when the maximum level of care and security is taken, there are risks that cannot be mitigated when data is shared. Being considerate about the ways risk factors may impact the security of data that is shared, and taking the time to think through multi-layered and contextually informed mitigation, are crucial steps in building robust and responsible data sharing practices and systems.

Annex:
Relevant technical approaches to risk mitigation, and how to evaluate these in context

Just as analysing risks related to data and technology involves paying attention to both environmental factors and technological factors, so does mitigating risks.

This section reviews **potential technological approaches to risk mitigation** that surfaced frequently in the research and/or that were identified by corresponding research commissioned by the DIGID consortium.[127] It offers an explanation of these technologies, discusses possibilities and limitations, and offers some key questions to answer when assessing security in individual contexts.

This section has been written specifically as guidance for decision-makers in the humanitarian sector who are involved in **designing, considering or evaluating** technical systems for data sharing; however, the explanations included could be of interest for anyone who wishes to better understand key approaches and terminology related to data security and privacy.

It should be noted that in any assessment or building of a specific system to share data, technical security expertise will be needed – both to make informed decisions and to make sure that the intended security protocols are implemented properly.

"Technology won't solve the problem"

As mentioned in the body of this report, when looking at mitigation in the context of data sharing, data can not be protected from the recipient; as such, risk in this scenario can always only be mitigated to a certain degree. Noting this, some of those we spoke to in our research encouraged the sector to consider how humanitarian CVA can be facilitated in a way that minimises both collection and sharing of data as far as possible.

A number of interviewees who are engaged in the technical elements of humanitarian operations also said that data protection efforts would be more effective if directed towards improving general data protection knowledge in the sector, rather than towards highly technical solutions. A digital security expert at a humanitarian organisation told us that humanitarians were "not being taught enough about basics [like] don't share passwords, etc."[128]

These interviewees pointed to the importance of understanding basic data sharing protection principles such as controlling access to data, ways to share data safely and the importance of data minimisation.

[127] Caribou Digital, "Investigating Safe Data Sharing."

[128] Interview with digital security expert at humanitarian organisation

Purpose limitation can be a key mitigation strategy when designing systems

Taking the complex nature of humanitarian work into account, more than one of the experts we spoke to for this research advised leaders in the sector to **limit technical solutions to *specific purposes*** as much as possible, as failing to do so can introduce unnecessary risks and complications into individual scenarios.[129]

More than one tech and data expert we spoke to noted, for example that[130] **deduplication** in particular could be done in ways that leave the data more protected. Two examples of this were mentioned:

- **Technically, through a purpose-limited system** that could allow a humanitarian actor to reference other datasets without having direct access to it ("'Is X in your database?' might, for example, be the only question that you need answered"). [131]
- **In-person deduplication:** One interviewees we spoke to said they had worked in operations where "organisations would come sit together in a room, bring their data, compare it and each one leaves marking those who they are assisting and who the others are assisting."[132]

Build in both data minimisation and least privilege

- **Data minimisation involves not collecting any data that's not absolutely necessary to collect.** In interviews, the importance of data minimisation came up repeatedly. As one interviewee noted: "As a rule of thumb, take as a starting point: only collect what you need. This is data minimisation. Once you have data, you have an obligation to protect it." [133] This sentiment was echoed in a number of interviews, and included minimisation in sharing, including how much is shared and what form data is shared in.[134]

  In terms of building data minimisation into a purpose-limited system, one interviewee advised: "Take a step back and ask – can we do something about [the problem identified] without creating too many records of information? What is the minimum number of things that can happen in the system for that to happen?[135]
- **The principle of Least Privilege** states that users of a system, or more generally, components of a system, should only have access to the smallest set of information that they need to perform their tasks. As a result, the harm that can result from, say, data leakage, is minimised.[136] As one interviewee said: "Know how the system is going to be working – both how it's designed but also how permissions are going to be managed.

[129] Interview with digital security and privacy researcher

[130] Interview with digital security expert at humanitarian organisation; Interview with digital security and privacy researcher

[131] Interview with digital security and privacy researcher

[132] Interview with information management expert at humanitarian organisation

[133] Interview with privacy expert and advocate

[134] Read more on data limitation for donors: IFRC, "Practical Guidance."

[135] Interview with digital security and privacy researcher

[136] Jerome H. Saltzer and Michael D. Schroeder, "The Protection of Information in Computer Systems," Fourth ACM Symposium on Operating System Principles (October 1973), https://www.cl.cam.ac.uk/teaching/1011/R01/75-protection.pdf.

> This involves working through the scenario of who will be accessing the data, how, and having mitigation strategies at every point."[137]

Cryptographic building blocks can be used to help to protect data from third parties, and/or to design purpose-specific solutions

Cryptographic techniques to protect data are difficult to do correctly, but if done well can provide more protection than can be achieved without them.

Cryptographic techniques can be used to help protect data from third-party access, but they could also be used to design solution-oriented systems for specific purposes that provide much stronger protection and do not involve sharing data at all. A system proposed by Wang et al, for example, provides a strong digital audit record without gathering data about transactions of identified individuals.[138]

At a high level, the following would be needed for the use of cryptographic building blocks to be successful:

- Decentralise data as much as possible
- Careful consideration of the roles assigned to different parties, and
- Careful consideration of all the assumptions that would guarantee this protection.

This section outlines a few key cryptographic techniques that can be used to help protect data in various scenarios, and looks at what scenarios each might be good for, and where its limitations are.

Cryptographic tools to protect data stored on third-party platforms and in transit

Several cryptographic techniques can help to protect data when this data is outsourced to a third party.

Standard Encryption

Standard encryption schemes (such as AES) can be used to protect data while it is stored with a third party, or to protect it in transit.

Symmetric encryption schemes use a secret key to encrypt data. Parties that do obtain encrypted data but do not know the secret key cannot learn anything about the underlying plaintext data. In general, it is recommended to use authenticated encryption schemes.

Encrypted data can safely be stored with a third party, as they cannot access it – however, ***the protection of encryption is only as strong as the protection of the secret key***. Anyone who holds both the encrypted data and the secret key can freely access the underlying plaintext data.

Asymmetric encryption is an alternative to symmetric encryption. Here, two different keys are used. The encryption key (sometimes called public key) can be used to create encrypted data.

[137] Interview with privacy expert and advocate

[138] Boya Wang, Wouter Lueks, Justinas Sukaitis, Vincent Graf Narbel, and Carmela Troncoso, "Not Yet Another Digital ID: Privacy-preserving Humanitarian Aid Distribution," *2023 IEEE Symposium on Security and Privacy (SP*), (2023), https://doi.ieeecomputersociety.org/10.1109/SP46215.2023.00174.

Typically, the encryption key is not secret – it can even be made public. Decrypting data, however, requires the corresponding decryption key (sometimes called secret key).

In a context where an organisation wants to **store encrypted data** on a third-party platform, for example, it would need an application that would:

1. Use the organisation's encryption key (or secret key, if using symmetric encryption) to encrypt the data locally.
2. Upload the encrypted data to the third party for storage.
3. Re-download the encrypted files when needed, using the decryption key (or secret key, if using symmetric encryption). In many cases, this process happens transparently, without specific intervention from the user.

The downside of using standard encryption techniques to store data with a third party is that **the data must always be re-downloaded before it can be read or operated on**. This approach can become problematic for large datasets that cannot easily be downloaded in the field.

End-to-End Encryption (E2EE). Often, encryption is used to secure data that is transferred *between two parties or end points.* We speak about end-to-end encryption when only the sender and the receiver are able to decrypt it (i.e., have the corresponding decryption key). In particular, when using E2EE, third party providers involved will not be able to access the raw data being transferred across their infrastructure. While not common, **some E2EE systems do exist for email, file transfer, and cloud file hosting** (*s*ee the box in Section 3: General ways in which data can be compromised) – however, it should be noted that these systems can be more challenging to use than the standard tools.

For example, to communicate securely using E2EE, two humanitarian organisations might proceed as follows:

1. The sending organisation obtains the receiving organisation's encryption key. It is essential that this encryption key is correct. If this encryption key could be substituted by a malicious intermediary, the guarantees of E2EE might completely fail.
2. The sending organisation uses this encryption key to encrypt the data that it wants to send to the receiving party.
3. The receiving party uses their decryption key to decrypt the encrypted data.

(This example relies on asymmetric encryption. Alternatively, the two organisations could directly agree on a secret key that they securely share between themselves.)

When the security and privacy properties of a system rely on encryption, it is helpful to ask:

- **Who has access to the decryption or secret key?** If at any point the third party that holds the encrypted data can also obtain the decryption key, the use of encryption offers much less protection.(Sometimes third parties can access decryption keys to offer data recovery abilities.)
- **When using asymmetric encryption, can we be assured we are using the right encryption key to encrypt the data?** And how is this guaranteed? If we accidentally encrypt using somebody else's encryption key, then that party can decrypt our files. This question is particularly important when aiming to use E2EE between two parties. When relying on a 3rd party to provide the encryption key, the security offered by the E2EE channel is diminished.

Homomorphic Encryption

Homomorphic encryption allows data to be worked with in certain ways (say, adding a number of records to compute a daily total) *without the client having to download it or the third party having to decrypt it.* This is not possible with traditional encryption techniques.

By using new ways of encrypting data, the third party can "compute" on the data without ever decrypting it. Suppose, for example, that the third party holds transaction records where the transaction amount is encrypted using a homomorphic encryption scheme. The third party can now, by itself, compute the *encrypted transaction total* for a specific day by adding up all encrypted amounts. In doing so, it never learns any individual amounts. The client now only has to download the encrypted total (which is much smaller than individual records) and decrypt the result.

The main advantage of using homomorphic encryption as a way to outsource data to third parties is that the third party (assuming it has enough computing power) **can compute the data but does not learn anything about the data itself.** This also saves on costs, as the client does not need to pay for download or computation cost, and can instead retrieve just the results of the computation. (The use of homomorphic encryption does not, however, automatically rule out all types of leakage, as the third party still learns which computation is performed, and on which items.)

As an alternative to outsourcing, **homomorphic encryption can also be used to compute locally,** if an organisation is willing to pay for the storage, transfer, and computation cost**.**

Limitations: Homomorphic encryption can't be used in every scenario, as not all computations are easily done using this technique. *In theory*, newer homomorphic encryption schemes, so-called *fully-homomorphic schemes*, support every possible computation. *In practice*, some of these might be so inefficient as to be impractical. As a rule of thumb: the simpler the computation, the easier it is to compute it over encrypted data. *Partial homomorphic* schemes, for example, are often very efficient, but only support addition (or multiplication) of encrypted data. This is sufficient to compute the *sum of a list of encrypted items* (e.g. adding transaction amounts) or, with a little bit more work, to *compute the average*.

But it cannot be used to compute, for example, the *sample variance* of a list of items in the encrypted domain, as this requires additions *and* multiplications. *Fully homomorphic schemes* support more complex computations because they support both addition and multiplication. However, to remain efficient, most schemes *limit the number of multiplications*. The question of how to efficiently implement computations using homomorphic encryption (e.g. by limiting the number of multiplications so fast schemes can be used) is a matter of ongoing research.

Questions to ask when considering whether to use homomorphic encryption to outsource data to third parties:

In addition to asking the questions for traditional encryption (who has the decryption key, and can we be sure we are using the right key to encrypt?), when considering homomorphic encryption to protect outsourced data it is also important to ask:

- **Does it make sense to let the 3rd party compute?** Or would it be architecturally simpler to just re-download the data and compute locally?
- **How complex are the operations that we want to apply to the data?** And how diverse are these? In general, homomorphic encryption can be tuned to work for specific computations, but finding an operational point that works for many very different operations is much more difficult.
- **Do you have reasons not to trust the accuracy of the output?** For example, a misbehaving third party might use the wrong encrypted inputs, or simply produce a result ciphertext

with a wrong answer. While techniques to include verifiability exist in the research space, these are for now less common.

Cryptographic tools to avoid sharing data altogether

Sharing of data is often not the root goal; instead, data is shared only to achieve an underlying purpose: for example, deduplication of aid recipients. Cryptographic techniques can help to achieve purpose limitation by ensuring that the intended purposes are achieved without further exposing data.

Critically, all of these approaches require the design, implementation and deployment of new cryptographic systems. This can be done (and often to great benefit in terms of data protection), but it requires specific resources and academic expertise, including deep technical knowledge about how to think through such designs.

For any advanced cryptographic designs, it is helpful to ask a few questions.

- **Which assumptions are needed to ensure that the system is secure and private?** Cryptographic systems designs always make assumptions. Some of these might be very reasonable and non-controversial (e.g. that SHA2 is a secure cryptographic hash function) while others might be more difficult to achieve in reality (e.g. that two humanitarian organisations or their servers are not simultaneously compromised). The discussion of each specific tool highlighted below includes specific questions to ask for each one, when considering it as a building block in a system.
- **Do the participating organisations have the necessary technical expertise to operate complicated cryptographic software?** Cryptographic designs achieve security by distributing trust among parties. However, operating such systems requires additional effort to run custom software and platforms.

Homomorphic Encryption: Multi-Party Setting

Homomorphic encryption can also be used to combine and compute on data supplied by different parties. In this setting, a group of parties agree that they will each share encrypted data with a third party server. In the most common scenario, each party creates an encryption and decryption key, and then uses their encryption key to encrypt their own data. They would then upload the encrypted data to the third party server, which conducts the computation and then shares the **resulting** encrypted data with the original set of parties. Each party can then use their own decryption key to finally reveal the result.

The main advantage offered by homomorphic encryption lies in the fact that the server never has access to the decryption keys, but it can nonetheless compute and combine data from different sources to obtain new encrypted records. The parties involved also never have access to each others' data – only the results of the computations.

By way of a simplified example: Suppose different humanitarian organisations each hold their own *transaction records* for services or funds they distributed in a given region. They want to compute the *total transaction amount*, but do not want to reveal any information about individual transactions. They can instead share homomorphically encrypted transaction records > the third party then computes the encrypted total > then the organisations jointly decrypt this total.

Important questions to ask:

- **How will the parties contributing data decrypt?** This is a variant of the question: where is the decryption key? As a general rule, if a party's data is used in a computation, then probably that party should also be involved in decrypting the final result.

- Will anything go wrong if the result is incorrect? In many cases, the third party doing the computation can choose to compute alternative (simple) functions of encrypted data. Is there any reason to suspect that such an attack might happen? If so, additional verification checks might be needed.

Secure Multi-Party Computation

Secure multi-party computation (SMC) is a different general technique that can be used to again effectively compute data held by different parties. In the case of SMC, however, there is typically no third party involved, but instead the different participants each help with the computation. The cryptographic properties of SMC protocols ensure that only the results of the computation are revealed, but all data provided as input by each of the parties stay private.

An example from Estonia shows how SMC enables privacy-friendly applications.[139] Between 2006 – 2012, almost half of Estonia's Computer Science (CS) students dropped out. Universities hypothesised that this was because these students were hired early, to work. Validating this hypothesis would require information from the ministry of Education, which has data on which students are enrolled in CS programs, with data from the Tax and Customs Board, which has data on employment. Because combining these datasets runs contrary to data protection regulations, researchers instead used SMC. In the SMC computation, three parties participated: the Ministry of Education (inputting enrolment data), the Tax and Customs Board (inputting employment records) and a commercial technology company, ShareMind.[140] Because of the properties of SMC, only the final statistical result was revealed, and no other data was shared between any of these parties.

At the same time, deploying SMC can be expensive. It requires specific technical expertise and can be computationally costly. In the concrete case of the Estonian CS students, for example, these statistics took more than 2 weeks to compute on moderately powerful machines.

Important questions to ask

- Do the parties involved have the necessary computational power to run these protocols? SMC protocols place a high load on computing entities in terms of computation and communication resources (for example, in terms of bandwidth needed between nodes). Such resources are typically available in data centres, but might not be as easily available in the field.
- Can the majority of parties involved be trusted? SMC protocols make assumptions on how many of the computing parties can be compromised before the privacy guarantees fail. A common assumption is that the majority of the parties, for example 2 out of 3, are honest and not compromised, and that no parties are colluding.
- How will the parties agree on which computation to compute? Depending on the specific instantiation of the SMC protocol, one or several of the parties must agree on the computation to perform. Ideally all parties should agree (see also above about the verifiability of the output), but some SMC protocols do not require this.

Clean Rooms

In recent years, commercial operators have started offering data "clean rooms", in which the operator hosts data provided by different sources, and enables them to compute aggregated

[139] Dan Bogdanov, Liina Kamm, Baldur Kubo, Reimo Rebane, Ville Sokk, and Riivo Talviste, "Students and Taxes: a Privacy-Preserving Social Study Using Secure Computation," Proceedings on Privacy Enhancing Technologies, 3 (2016), https://eprint.iacr.org/2015/1159.pdf.

[140] "The next generation of data-driven services with end-to-end data protection and accountability," Cybernetica, accessed November 21, 2023, https://sharemind.cyber.ee/.

statistics on the combined data. What is less clear, however, is how these clean rooms function technically, and therefore what level of security guarantees they offer with respect to the data that they host.

A particular point of concern around clean rooms is whether the operator itself is able to access the data, or not. (Assuming the clean room itself is instantiated properly, protection against outside parties is relatively easy to achieve using standard cybersecurity practices.) If the clean-room operator can technically access the stored data, protection then relies on procedures and legal agreements. If, however, the clean room is instantiated using strong cryptographic methods such as MPC or homomorphic encryption, it is possible to make sure that the operator can never access the data itself.

In evaluating the security of specific clean rooms that do use strong cryptographic techniques such as MPC or homomorphic encryption, there are a few key factors to take into account:

1. Any system using these techniques properly can offer limited options in terms of what computations it can actually do, and broad claims around functionality may indicate less robust protection.
2. What the answers to the same set of 'important questions to ask' from the section above. In particular:
    - **For homomorphic encryption solutions generally: Who holds the corresponding decryption keys?** In secure instances, each data provider will normally hold a decryption key and will be required to help decrypt any computation results. If the data provider is not required to help decrypt, this is also a sign that perhaps the architecture is less secure.
    - **For MPC solutions: Which parties are computing?** Are these the data providers themselves? (If this is the case, they will be required to remain online, and participate.) Or other parties? If so, why would these then be trusted?

Other Cryptographic Tools & Strategies

Hashing

Hashing is sometimes advanced as a simple solution to data protection, but for hashing to be successful it needs to be used and analysed **in the context of the full system it is part of** – i.e. cryptographic hash functions are a building block that can be used inside larger cryptographic protocols.

A hash function maps random data (of any length) to a much shorter random-looking string. For example, the SHA-256 hash function will output 256 bits (32 bytes) of data, regardless of the input. Hash-functions are often used because it is difficult to "invert" them: given the output of a hash function, it is difficult to determine the corresponding input *assuming that the space of possible inputs is very large.*

Because hash functions guarantee that the same inputs/values are mapped to the same outputs, they are sometimes used to protect data fields before sharing them. However, it is still possible to link the dataset, and careful analysis is needed in any specific scenario to confirm that the use of hash functions does in fact increase security / privacy in that scenario.

By way of example: Two humanitarian organisations want to determine if they are providing assistance to the same people. To do so, each organisation takes the list of identifiers for their recipients, hashes each of these identifiers, and shares the list of hashed identifiers with the other organisation. Each organisation can now detect duplicates in their list of hashed values.

Because hash functions are difficult to invert, it might now be concluded that neither organisation learns anything about non-duplicate recipients aided by the other organisation, and nor could an attacker that gains access to the hashed lists. However, this is not in fact the case, as the set of possible identifiers is small and easy to enumerate – anyone wanting access to the 'unhashed' data would simply compute a dictionary of all possible identifiers and their corresponding hash value; and then lookup entries in this dictionary.

When using hash functions – for example to protect stored passwords – **manuals typically recommend using salts.** A salt is a long, usually item-specific, random string that is appended to the real input before computing the hash function. This makes the dictionary attack outlined above harder: the attacker now needs to compute a dictionary per entry to recover the original data. However, when the size of possible inputs is not too big, as in the previous example, this does not really matter.

Another technique that helps more, is to use a **secret salt**, or **pepper**, that is only known to (taking the example above) the two humanitarian organisations checking for duplicates. As with a salt, this secret salt is appended to the input before computing the hash function. An attacker that obtains the hashed list, *but not the secret salt,* can no longer even compute the hash values, and thus cannot build the dictionary or invert the hash function.

The protection provided by this approach, however, crucially depends on the fact that *the attacker cannot obtain the secret salt*. In the above example of comparing two lists, both organisations still need to know the secret salt, so an attacker could obtain this value together with the database. Moreover, the use of a secret salt does not provide any protection if the concern is that the other organisation itself might not have sufficient levels of data protection to protect both the data and the secret salt.

Decentralising data through the recipients of assistance themselves: digital wallet solutions

An alternative approach to directly transferring data about recipients between organisations is to rely on the recipients themselves to make the transfer. This is commonly seen outside the humanitarian sector in areas where people are issued official documentation: For example, a citizen might use their driver's licence to convince others that they are allowed to drive a specific vehicle, or show their degree to convince an employer that they have obtained the necessary level of education.

This type of analogue data transfer can also be done in the humanitarian sector. For example, in the case of a referral, an organisation that registered a beneficiary could provide that recipient with a document containing all relevant information. The recipient could then provide this document to the relevant other organisation themselves. (It should be noted, however, that while this approach avoids having to obtain all information from the beneficiary again, it might still require the target organisation to re-enter the data. Standardisation of data formats can ensure data can be integrated efficiently at the target organisation.)

At the extreme end of systems that place recipients in control of their data are digital wallet solutions, such as those proposed by the DIGID consortium.[141] In these systems, recipients manage their own data and can choose to share it with humanitarian organisations when asked. From a functionality point of view, such systems are similar to the paper-based systems described above, combined with a specified data format, and protections against tampering. As such, they can be used in referral settings. It is unlikely, however, that this approach is effective in deduplication settings, as users could always claim not to have been registered yet. (Checking the validity of this claim is as hard as the original deduplication problem.)

[141] "DIGID: Dignified Identities in Cash Assistance," Humanitarian Innovation Platform, accessed November 21, 2023, https://hiplatform.org/digid.

The security and privacy benefits of digital wallets are hard to assess without looking at the details of specific systems. When implemented well, the data can only be accessed by the recipient themselves, and recipients have full control over which data they share with humanitarian organisations. In practice, this would require recipients to manage their data on their own devices, maintain secure access tokens, and/or remember complex passwords. Therefore, realistic deployments might be much less secure. Depending on the setting, organisations might also be able to access all data (instead of only a subset), and/or the operator of the system might be able to access data as well due to a recovery mechanism.

Blockchain

Another building block that is sometimes mentioned in the context of digital systems are blockchains. The core function of a blockchain is to create an immutable ledger. Traditionally, this ledger contains a sequence of transactions, but more recently blockchains have been used to create an immutable record of many different types of actions and pieces of information.

All blockchains ensure immutability of the ledger by relying on a 'distributed trust' assumption: The ledger is maintained by a set of parties, and as long as a sufficient number of these parties is honest, the records cannot be modified.

Different designs provide different trade-offs:

- In **permission-based blockchains,** a *limited number of trusted parties* maintain the blockchain.
- In **permissionless blockchains**, *anyone* can participate in the maintenance of the blockchain (e.g. through mining blocks).

Not only do permissionless blockchains tend to be less efficient than permission-based blockchains, but the data on permissionless blockchains (e.g. the ledger) *has to be* public in order to allow any party to help maintain the blockchain. This makes it difficult to guarantee privacy. In the **permission-based setting,** typically the trusted parties have to have access to all the data, but data on the blockchain can be hidden from unauthorised parties.

Blockchains for immutable logs

The core strength of blockchains lies in their ability to provide immutable records even when not all the parties involved can be trusted. In a humanitarian setting, for example, they could be used to store access logs of which person or organisation accessed what data. The immutability of the block chain ensures that later modification of the log file is not possible. In the case of unauthorised access, these logs could then provide evidence of such access. However, in this scenario, three important questions must be asked:

1. **Do the extra immutability guarantees of blockchains really help?** Blockchains guarantee that logs cannot be modified even in the face of misbehaving or malicious participants. But to ensure safe logging, it might suffice to just send logs to one or more other parties for safe keeping.
2. **Can we guarantee that logs are always written?** If incidents of unauthorised access are not logged – for example because an attacker prevents that – then the logs themselves, however trustworthy, are not useful. More advanced systems based on blockchains therefore integrate access control into the blockchain mechanism, thus ensuring that first retrievals of data are always logged.
3. **Do we also want to detect access to data that organisations legitimately have access to?** If this is the case, trusted logging is likely not going to help detect this. If a user or organisation legitimately accesses data to perform their day-to-day humanitarian tasks,

then any attacker that gains access to their systems can access sensitive data on that system *without triggering any logging mechanism.*

Finally, trusted logging, or immutable ledgers more generally, do not help prevent unauthorised access. They can only, in some cases, help reveal that such access took place.

Decentralised Registries. Distributed ledgers and distributed file systems (such as Interplanetary File Systems, or IPFS) are sometimes proposed as a way to create a decentralised or distributed database that can be accessed by multiple parties. This is most useful when the data or database cannot be hosted directly by a single entity (creating a single point of failure in places where access might be blocked by government censors, for example).

From a security and privacy standpoint, however, the advantages of distributed ledgers and file systems are unclear. If data is being stored unencrypted, these systems might actually make it *easier* for unauthorised parties to access data, to observe metadata, and to observe access patterns than it would be if a single party were hosting the data.

Ledgers and distributed file systems, by design, do make it easier to guarantee integrity of the data. But if integrity is a primary concern, standard techniques can ensure integrity of data when hosted by a single party as well.