



Practical Guidance for Data Protection in Cash and Voucher Assistance

A supplement to the Cash in Emergencies Toolkit

January 2021

Contents

I.	Introduction	4
	Target Audience & Document Purpose	4
	Structure of this Document	4
II.	Data Protection Overview.....	5
	Processing Personal Data.....	5
	Legitimate Basis	5
	Key Data Protection Principles.....	6
III.	Targeting	7
	Personal Data Use.....	7
	Data Protection Considerations.....	9
	Project Decision 1: Should I use beneficiary data collected by an external source?.....	9
	Project Decision 2: How do I verify the eligibility of beneficiaries?.....	11
	Project Decision 3: Should I talk to beneficiaries about the handling of their data at this stage?	13
IV.	Beneficiary Registration.....	13
	Personal Data Use.....	13
	Data Protection Considerations.....	14
	Project Decision 1: How should I verify the identity of a beneficiary?	14
	Project Decision 2: What other data should I collect from beneficiaries during registration?	16
	Project Decision 3: What should I tell beneficiaries about the handling of their data?	19
	Project Decision 4: Should I ask beneficiaries for consent?.....	21
V.	Use of Financial Service Providers	23
	Personal Data Use.....	23
	Data Protection Considerations.....	24
	Project Decision 1: Should I use a Financial Service Provider?.....	24
	Project Decision 2: Which account type should I choose for the cash distribution?	26
	Project Decision 3: What should the contract with an FSP contain?.....	27
VI.	Data Sharing with Government, other Humanitarian Organizations, and Donors.....	28
	Personal Data Use.....	28
	Data Protection Considerations.....	28
	Project Decision 1: Which data should I share with government?.....	29
	Project Decision 2: Which data should I share with other NGO's?.....	30
	Project Decision 3: Which data should I share with donors?	33
VII.	Post-Distribution Monitoring.....	34
	Personal Data Use.....	34

Data Protection Considerations	34
Project Decision 1: What personal data should I collect in the monitoring process?	34
Project Decision 2: What beneficiary data can the FSP give me to monitor my programme?	36
Project Decision 3: What beneficiary data can the merchant give me in a voucher programme?	39
VIII. General Guidance	39
Data Protection Considerations.....	39
Data Storage.....	39
Data Retention and Deletion	40
Access Control.....	41
Transmission process (Data sharing)	42
Handling of Data Breaches.....	43
Briefing of Staff and Volunteers.....	44
Analysing and Monitoring Data Protection Risks.....	44
Community Engagement and Accountability (CEA).....	46
IX. References	47

I. Introduction

As the International Red Cross and Red Crescent Movement implements its commitments to scale up Cash and Voucher Assistance (CVA), it also increases its collection and processing of personal data, particularly those of the vulnerable communities being served. Data protection is not only a matter of good governance; it is also about building trust. In times of crisis, beneficiaries may be thinking about more urgent priorities necessary for their survival and safety than risks to their personal data provided to aid organizations. This is even more reason for cash practitioners to respect and be responsible for the protection of beneficiary data. Additionally, other stakeholders such as donors, government entities, and other partners will have increased confidence in our CVA programs when good standards and practices for data protection are demonstrated.

Target Audience & Document Purpose

This practical guidance is intended for **cash practitioners** or those managing programmes to embed data protection principles in their implementation of CVA. There are many useful data protection references available for humanitarians, including the [Handbook on Data Protection in Humanitarian Action](#) and the respective Data Protection policies of the [IFRC](#) and the [ICRC](#). While those references are more general in nature or only address some of the issues facing cash practitioners at a high-level, this document aims to translate general data protection principles into practical, actionable guidance, specific to key activities in the CVA process. This guidance will provide key considerations on data protection and guide cash practitioners in their decision making and implementation.

This document references the processes in the [Cash in Emergencies toolkit](#) (CiE) and will supplement the toolkit until it is revised to directly include the data protection considerations explained in this document.

IMPORTANT:

This guidance is to be contextualized by the National Societies to meet requirements unique to them; in particular, adherence with their national data protection laws and policies which might be stricter than the standards of data protection applied here.

Structure of this Document


The next section will provide an overview of Data Protection to introduce readers to the key principles and terminologies that will be used in the guidance. It will then be followed by chapters for each of the five key processes for CVA.

Before developing this guidance, an analysis of the CiE toolkit was done to identify the processes where beneficiary personal data is collected and processed. The processes were then prioritized based on the level of processing of personal data and potential risks. This guidance will focus on five of these priority processes¹:

1. Targeting
2. Beneficiary Registration
3. Use of Financial Service Providers
4. Data Sharing with Governments, other Humanitarian Organizations, and Donors
5. Post-Distribution Monitoring

¹ This aims to be a living document and practical guidance for other areas of the CiE toolkit may be developed in subsequent revisions as we grow in our experience in data protection.

Each chapter will have an overview describing how personal data is used or processed with examples based on consultations with National Societies. It will then be followed by a set of data protection considerations based on key project decision or questions.

Each consideration starts with a box highlighting a key project decision or question. A bell icon  indicates which data protection principles are relevant to the consideration. A framing of the relevant project question is then provided to incorporate the data protection consideration. Those considerations are explained in more detail and accompanied by simplified examples to demonstrate how to apply the considerations.

The last chapter is for General considerations that are applicable for the entire CVA programme cycle.

II. Data Protection Overview

Processing Personal Data

What exactly is personal data? **Personal data** is any information that may lead to the identification of a living, natural person (the data subject). Data can be personal even if at first glance they may not seem to be tied directly to a person but could lead to identification indirectly by using additional information. This may sound complicated, but it basically means that data protection covers a broad range of information, and that the term “personal data” should not be interpreted in a narrow way. In the context of CVA most data you will collect from beneficiaries will qualify as personal data, for example:

- Names and contact details
- ID numbers
- Bank account numbers
- Employment details
- Family situation
- Health condition
- Address or geolocation

On the contrary, data that you collect to analyse the situation on an **abstract level** (e.g., economic information of the region, etc.) do not generally qualify as personal data. This data is anonymous, because it does not deal with people’s information at all, or that the information is in aggregated form. **Aggregated data** is data that is created by summarizing and combining individualized data. Individuals are not identifiable in aggregated data (neither directly, nor indirectly), which typically provides a general overview using charts, tables, statistics, and general information about groups of people, not individuals. Examples include statistics on types of livelihoods, average household size or income, percentages on damage to shelter within an area, or the calculation of minimum expenditure basket (MEB).

The **Processing** of personal data essentially means anything you do with the data, such as collecting, storing, organising, sharing, evaluating, modifying, publishing, recording, using, correcting, and even deleting it.

Legitimate Basis

All processing of personal data requires a legitimate (or *legal*) basis. A commonly used legitimate basis is Consent. However, there are various other grounds to legitimate processing of personal data, including:

- Compliance with a legal obligation
- Performance of a contract with the data subject

- A task in the Public interest
- Vital interest(s) of a person (near-term threat to their mental or physical health)
- Legitimate interest of the entity (it could be IFRC, ICRC, a National Society, for example) processing the personal data

Which legitimate basis to rely on can sometimes be challenging. More details on the definition and differences of these legitimate bases can be found in the [IFRC Policy on Data Protection](#) and the [Handbook on data protection in humanitarian action](#) by ICRC and Brussels Privacy Hub.

For CVA it is quite common to rely on consent. Many cash practitioners include a consent question at the beginning of a survey or data collection form. However, for emergencies this is not necessarily the best option. This is explained in more detail in the Beneficiary Registration chapter with a decision tree to help evaluate whether one or more other legitimate bases may be more appropriate under the circumstances.

Key Data Protection Principles

There are several data protection principles to consider when processing personal data. Although the names may change depending on the policy or international instrument, it is generally accepted that the main data protection principles are: (1.) lawfulness, fairness and transparency; (2.) purpose limitation; (3.) data minimization; (4.) accuracy; (5.) storage limitation; and (6.) integrity and confidentiality (security). You can find more detail about them in the [IFRC Policy on Data Protection](#) and the [Handbook on data protection in humanitarian action](#).

However, for the purposes of this guidance, we will focus on the principles most relevant to CVA (noting that the principle of lawfulness, or “legitimate basis”, has already been discussed above). Principles will often be discussed together where they should be jointly considered to make the relevant data protection analysis, even though strictly speaking they are considered distinct principles. For instance, in the next section we discuss two distinct principles “data minimization” and “purpose limitation” together, because it is not possible to evaluate what data is necessary without an assessment of the purpose(s) of the data collection/processing.

Data Minimization, Necessity and Purpose Limitation

The data minimization principle means, “collect as little as possible and ONLY as much as necessary.” To define what is necessary, it is important to clearly identify the *purpose* for which the respective data is to be used. In the context of CVA, the processing of personal data may serve various purposes (e.g., check against targeting criteria, verify identity, facilitate cash distribution, to detect or avoid fraud, and monitoring programme impact). The processing of personal data must be *necessary* to achieve the respective purpose. Before collecting information, it is crucial to understand what information is needed in the specific context. If you are unsure why you are collecting a particular set of data or think that it may come in handy later without specific rationale, or simply think that the more data you collect from beneficiaries is better, then you are probably going to collect more personal data than is strictly *needed*. To clearly identify what data is necessary, it is suggested to review data minimization / necessity / purpose limitation principles. These issues are fundamental to data protection and will come up often in this guidance. More details and relevant examples are provided in the Targeting chapter.

In addition, personal data collected for one purpose cannot simply be used for any other purpose. Of course, an existing data set may be used for future purposes under certain circumstances. However, the future purposes generally must be “compatible” with the original purpose. Such compatibility exists where the purposes are closely related, and it can be assumed that the data subject would not be surprised about this secondary usage. For example, at the end of a CVA programme additional

funds become available that were not previously expected. A review of the previously collected beneficiary data to determine whom should receive new assistance would be considered compatible with the purpose and the legal basis upon which the personal data was previously collected. Otherwise, an appropriate legal basis would need to be identified and the data subjects may need to receive updated information about the intended further use (see next principle of Transparency).

Transparency

Transparency goes together with fairness. The idea is to be open and honest about the handling of the personal data. Under the transparency principle, data subjects should always receive certain key information about what is happening with their data, including:

- the fact that their personal data is being processed and the basis for such processing
- who will be processing the data
- for what purpose(s) the data are processed
- how the data is stored and for how long
- if their data is intended to be shared with another entity
- the rights they have relating to the processing, such as right to correction and deletion
- contact details or someone to go to in case the data subjects have questions or complaints

The form in which this information is provided depends on the context. Specific examples will be given throughout the guidance.

Data Security (Confidentiality, Integrity, Storage Limitation)²

Personal data must be treated confidentially and securely. This might be obvious, but it is not always clear what needs to be done to ensure confidentiality. Data protection law (or policy, where applicable) requires the implementation of various security measures, such as access restrictions and data loss prevention. The ultimate goal is to avoid data breaches, meaning *the unauthorized access to, or destruction, loss, alteration or disclosure of personal data*.

III. Targeting

Personal Data Use

Targeting of cash assistance is informed by the programme objectives based on assessed needs. It aligns programme activities to specific beneficiaries using defined targeting criteria, which typically includes socio-economic and vulnerability indicators. See section M3_3 of the CiE toolkit for more details.



Figure 1: Steps in the Targeting process

The general steps in the targeting process are shown in *Figure 1*. This process may rely on previously collected data to inform the criteria setting and speed up the creation of the preliminary list of beneficiaries eligible for CVA assistance.

Steps 1 to 3 walk through key decisions in targeting based on programme objectives. Such decisions include:

²Storage limitation is normally considered to be a separate principle.

- Which geographic locations will be selected for the intervention?
- Blanket versus targeted distributions?
- Whether to target households or individuals?
- Which targeting criteria to choose based on vulnerability, socio-economic, or context specific inputs?
- Which targeting mechanism to choose (categorical, self-, or community-based targeting mechanism)?

In general, personal data does not play a significant role in these first three steps. Decisions are based on general information or aggregated data on the affected areas and population as a whole. Here the individual situation of potential beneficiaries is not yet of interest, but rather the overall situation on the ground and programme objectives.

Steps 4 and 5, however, do deal with personal data as potential beneficiaries are analysed, checked against the criteria that have been set, and a preliminary beneficiary list is created before the formal beneficiary registration process. The list will contain beneficiary names at minimum, and the analysis or verification process may involve detailed information about the beneficiaries.

In Step 4, the preliminary list is typically developed based on the targeting mechanism decided on Step 3:

- **Community-based targeting** – vulnerable households identified by community leaders and members based on the agreed criteria; results triangulated and verified by the National Society. E.g., community leaders asked to identify the households that had totally destroyed homes.
- **Self-selection targeting** - individuals are asked to provide information about themselves and details related to the agreed criteria. E.g., programme team looks for food insecure, able-bodied adult willing to participate in a Cash for Work programme.
- **Categorical targeting** – eligibility is based on specific categories of vulnerabilities (e.g., child-headed households) and potentially a good civil registry to decide which individuals belonging to a specific category to select. E.g., local government officials are asked to share a list of community members in extreme poverty.

Regardless of the targeting mechanism used, this step relies on data gathered from different sources (e.g., government, local communities, other organizations, or individuals). Although the initial list may be obtained from another source, the act of taking this list already qualifies as usage of personal data. If there is no initial list available, the National Society may opt to go door-to-door in the affected communities to develop such a list asking for personal data.

In Step 5, the eligibility of all persons named on the preliminary list is verified. This process might involve community representatives or local leaders that have current knowledge of the population or have compiled information using other data or systems (e.g., civil registry or social protection lists). In certain cases, a National Society may go door-to-door to check directly with the beneficiaries to verify that they are indeed eligible based on personal data they provide. The process for this door-to-door verification maybe done in parallel to the creation of the initial list per Step 4. This verification process might be similar to the beneficiary registration process and may use survey forms and a database to collect and manage structured personal data or could just be ad hoc using pen and paper to tick the criteria that the beneficiary meets--this is also considered personal data.

At the end of the targeting process, the list of verified beneficiaries may be shared and published in the community (i.e., list is printed and posted in a public space for the community to check who is included in the intervention). The publication of this list qualifies as using (processing) personal data,

because you make data in your control accessible to others – to all community members, so that they can evaluate the list.

Data Protection Considerations

The targeting process will involve the processing of personal data when setting up the preliminary beneficiary list and when verifying such list. This section will look at key project decisions in the targeting process and the considerations related to data protection. The most relevant principle this section will deal with is **data minimization/necessity**. All other principles relate to the handling data you have collected, while data minimization and necessity aims to limit the collection of data in the first place. Not to collect data you do not really need for the programme is the most effective way to increase the level of data protection. Hence, when setting up the programme and before you collect any data about beneficiaries, it is key to think through the programme life cycle and to decide in advance which data will be necessary throughout the programme.

Project Decision 1: Should I use beneficiary data collected by an external source?

 Data Minimization, Necessity and Data Security

Project Decision reformulated: Do I need the data collected by an external source and how can I make sure the beneficiary data has been collected in an appropriate manner?

When creating the preliminary beneficiary list, it is common to use beneficiary data from external sources such as other organizations or the government. So, the project decision question may seem obvious and necessary. However, the reformulated project decision question recommends cash practitioners to take a nuanced approach to asking for and using data from external sources that keeps in mind data minimization and data security principles, particularly when there are no established data sharing agreements.

Here are key things to consider when thinking to use beneficiary data collected by external sources (other NGO's, government, etc.):

- **Is this organization reliable and can I trust its data?** If the organization offering the data is not well-recognized, you may want to ask or investigate how they have collected their data, and would you consider this reliable? The concern here is not only that the data may be incomplete or incorrect, but also that data may have been obtained inappropriately (e.g., not having a clear legal basis or beneficiaries were not informed how their data will be shared with others especially if they are very sensitive). Depending on the context it would help to ask community leaders or other organizations active in the area whether they know and trust this organization. It is also advisable to ask the organization to give you some information on how the collection took place. It is important to know whether beneficiaries are aware that their data might be shared with you. If you doubt that things were done as properly, this is an indicator that you might want to consider other data sources.
- **Which data do I request and accept?** Because another organization has collected a certain amount or type of data, this does not mean you should take **all or most** of it. Again, the principle of data minimization and necessity is good to reflect on. It depends on the project, which data you should request or accept. If the other organization provides you with more data than you need, it is advisable to ask only for that data and if unneeded data is provided

delete that data and inform the other organization, so they are aware of what has been retained. Caution is recommended if the data set contains very sensitive categories of data, such as health, sexual or religious information, especially if this data is not directly relevant for your programme needs. Having an organization freely provide these types of data with or without formal data sharing agreements could indicate that they have poor or no data protection standards. Furthermore, data received from externals should be treated responsibly.

The scenario described above does not involve data sharing agreements between the parties and therefore control of data becomes an important consideration. For CVA programmes where the National Society is an implementing partner of another agency, the data exchange should be agreed between the involved partners, external or otherwise, and these considerations may be evaluated when negotiating the data sharing agreement. If, in the context of those cash programmes, you are concerned about data protection with regard to the data sharing with externals, please communicate your concerns with your manager or legal team within your National Society and note the risks/concerns in your CVA risk matrix.

Examples:

Target criterion is “households with children who lost their homes in the flood”.

The National Society team puts a request to the local government to provide:


- “relevant information” on residents of the area. This request is very broad, and it is likely that the government will provide more information than needed. This request should be narrowed down.

- “the names and family status of all the residents of the affected areas”. This request is more specific, but still too broad. Persons without children are not targeted. Hence, their names are unlikely to be necessary.

- “only the names of such residents in the affected areas who have children”. This is likely to be necessary and sufficient.

In the aftermath of an earthquake the National Society tries to identify the people that have lost their homes. An association in the most affected village offers to share a list of persons currently without shelter due to the earthquake. The National Society considers this offer carefully. They contact the mayor of the village and asks about the association’s reputation. Furthermore, they contacted the association regarding their data collection procedure. The association explains that they have informed people about data protection and about the intention to share data with other aid organizations. The data collected by the association included names, size of the family, age of the children and a mobile number. The National Society plans a blanket distribution for all households having lost their home. Consequently, they decide that for their intervention they only need the names of the beneficiaries and their mobile numbers to contact them. The team makes sure to receive not more than this data.

Project Decision 2: How do I verify the eligibility of beneficiaries?

 Data Minimization, Necessity, Confidentiality

Project Decision reformulated: Which data do I really need to verify the eligibility of beneficiaries?

The purpose of the verification or “eligibility check” is to find out whether a person (or household) actually meets the target criteria. This is typically done in **Step 5** of the targeting process mentioned above where it might be necessary to gather or analyse data related to the beneficiary. When doing this verification, it is important not to collect or process more data than is needed to complete the task (principle of data minimization and necessity). Different methods could be employed to check eligibility and they may require or process personal data differently:

- **Using community members for verification.** In this method, actual beneficiaries might not yet be consulted directly. Rather, community members that have knowledge of the situation or personal details of the beneficiaries might provide a preliminary list of potentially eligible beneficiaries. This could be followed up with a more formal verification check during the beneficiary registration process. When using this method, it is important that the privacy of the beneficiaries is protected, especially if the method is done in a public setting (i.e., with other community members) and since the actual beneficiaries cannot object to sharing information that others already know about them. Questions asked of the community leaders on data about the beneficiaries should be minimized and sensitive questions should be avoided in a public setting. If any information that could be deemed sensitive is required for the programme, try to only collect such information in a private setting, door-to-door verification, for instance.
- **Door-to-door verification.** Before actually visiting the beneficiary households to check their eligibility, it is important to identify what data is absolutely necessary for this purpose, again respecting the principle of data minimization and necessity. Since the efforts in going door-to-door could be high, there may be a tendency to ask for more information than is strictly necessary, in order to avoid having to repeat a visit. Therefore, preparation as to the scope and purpose of the programme is essential, so as to ask only the absolute minimum needed for the verification. If you are uncertain whether you should ask for a certain information, ask yourself the following question: what impact will the information have on my decision to target the individual beneficiary? If you are unsure, it may not be necessary.
- **Publishing the preliminary beneficiary list.** As part of Step 4 or after Step 5 in the targeting process shown above, the list of preliminary beneficiaries is typically shared and published in a public setting (e.g., community hall). This is to create transparency and to inform the community who has been selected based on agreed targeting criteria. It also gives an opportunity for those who are not on the list but meet the targeting requirements to be included in the programme. This list will contain personal data, so it will be important to minimize what is shared publicly. Typically, the names and general location are enough, and details or data used in the targeting verification are not necessary. However, knowing that the list of names is tied to some defined criteria (even if the details of which criteria may or may not be met), it tells the wider public something about the listed individuals that could be problematic for their privacy. Whether this is problematic from a data protection point of view, depends on the context. In a small village where the living conditions of all residents are common knowledge anyway (meaning that they have or have not the characteristics that

correspond with the target criteria), the publication of the list may not be as problematic in terms of privacy. On the contrary, in a context where beneficiaries live in relative anonymity, the publication of the list could be an issue. The release of information that was not publicly known before is likely to conflict with the principle of confidentiality. Hence, it is advisable to carefully consider the context before deciding whether to publish the list or not.

Additionally, after the verification or eligibility check process, data of those that were deemed not eligible should be treated responsibly (for example, archived securely if there are audit requirements, a simplified list maintained in order to avoid re-verification, or deleted if no longer needed). More details on this can be found in the General Guidance Chapter.

Examples of necessity and minimization during eligibility checks:

In the context of a programme, the target criterion is “households taking care of persons with disability”. For the eligibility check it is necessary to know whether there are actual members with disability living in the same household. It may be relevant to know the nature of disability they have. When verifying the facts this will be revealed during the house visit, for instance. However, most likely it is not necessary to consult the medical records to verify the disability and doing so could reveal sensitive personal data that is not relevant to the programme.

Community leaders suggest targeting single mothers with at least three children and no income as the most vulnerable and a preliminary list is created based on this criterion. The information provided by the community leaders is verified during house visits where the beneficiary is identified and asked about the ages of all household members. To verify income, it could be necessary to ask about the beneficiary’s sources of income. However, it would most likely not be necessary to collect additional information such as her age or her religious affiliation, because this will not influence the decision to target this beneficiary. It is also not necessary to ask about previous employers or request for bank statements to determine income level.

In the context of a response to famine, the target criterion for the cash programme is “food insecure child-headed households”. It is unlikely to be necessary to ask about the children’s education level when doing the eligibility check. The education level will not influence the eligibility check or the amount of the cash grant.

Note: In data collection and any further data processing, it is important to recall that personal data must be handled securely. Whether data is collected on paper, a mobile application, or other means, ensure that data is only accessible to those that strictly need such access. Data security must be considered at all stages, including deletion of any data, to ensure that it cannot be recovered. More details on this can be found in the General Guidance Chapter.

Project Decision 3: Should I talk to beneficiaries about the handling of their data at this stage?

 Transparency

Project Decision reformulated: How can I make sure beneficiaries have access to information relating to the handling of their data?

An important principle of data protection is Transparency. In the context of the eligibility check, the collection of information may be less formal than the beneficiary registration. Nevertheless, it is important for the beneficiaries to know what is happening to the information they share with you. More details on how to inform beneficiaries are provided in the Beneficiary Registration chapter, however it is already good to observe these standards when doing verification or eligibility checks. Some things to inform the beneficiary:

- Where you got the primary information about them (e.g., via community members, government list, other organizations?)
- Why you conduct the eligibility check
- That inaccurate data may be corrected anytime
- That you might share the data provided with other institutions and for what purpose (if that is the case)

IV. Beneficiary Registration

Personal Data Use

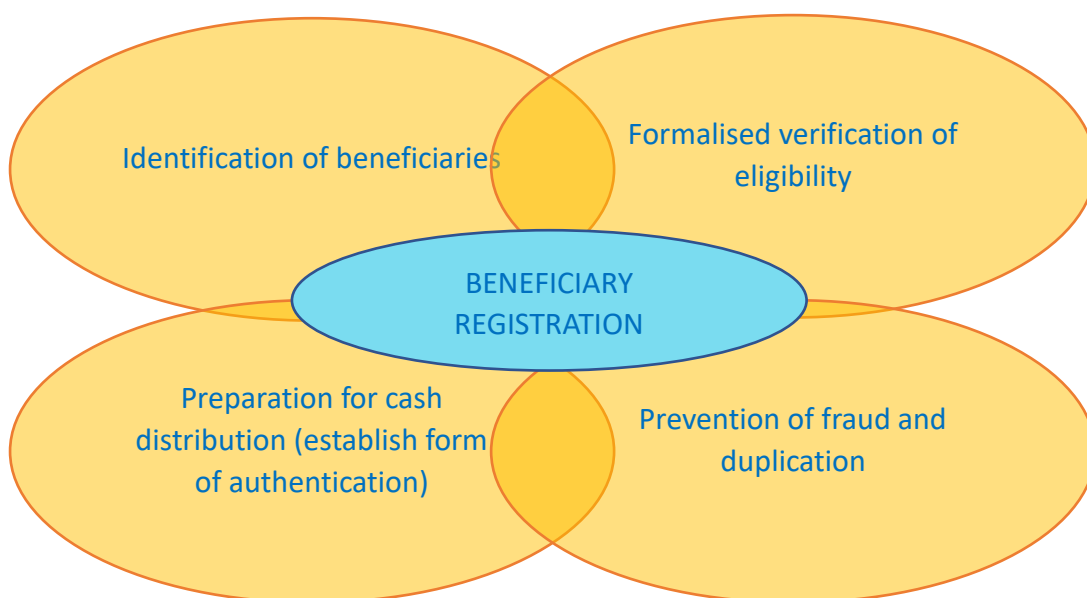


Figure 2: Purposes for conducting Beneficiary Registration

The process of formally registering beneficiaries typically happens after a list of eligible beneficiaries has been created (see section M4_4 of the CiE toolkit for more details). This involves collecting personal data and managing that data for distribution and monitoring of the programme. Figure 2


shows the common purposes for beneficiary registration and the examples below elaborate the use of personal data:

- **Identification.** At the beginning of the registration process, the head of household is typically asked to show an ID (e.g., driver license, tax or voting ID) to make sure they are the one included in the beneficiary list. These ID's will contain their name, date of birth, and other personal data that may be captured in the registration. The beneficiary may be asked to provide biometrics (such as a fingerprint) for strong authentication and to ensure that they were not registered multiple times. Biometrics is considered personal data and could be sensitive.
- **Formal verification of eligibility.** The beneficiary is asked questions related to the targeting criteria in case the verification process was not done formally before, and if there's chance that data may have changed since the targeting was done--to ensure the beneficiary is still eligible prior to cash disbursement.
- **Prepare for cash distribution.** Where applicable, the beneficiary is asked for Know Your Customer (KYC) or other information required by the financial service provider (FSP) to distribute money to them (e.g., mobile number for mobile money or bank account details).
- **Establish form of authentication.** The beneficiary is provided a Red Cross beneficiary card with their photo and a unique identifier that they could show the financial service provider as proof that they are eligible and have been registered. Particularly useful when official ID's are not available.
- **Prevention of fraud and duplication.** To prevent fraud and duplication, the beneficiary might be asked to provide personal data relating to family members or biometric data.

Data Protection Considerations

The beneficiary registration process will involve the collection and processing of personal data based on the common purposes described above. This section will look at key project decisions in the registration process and the considerations related to data protection.

Project Decision 1: How should I verify the identity of a beneficiary?

 Data Minimization, Necessity

Project Decision reformulated: Which verification mechanism is effective and interferes the least with the interests (including privacy) of the beneficiaries?

To verify the identity of the individuals showing up for registration, a unique identifier is required. Unique identifiers can be paper based (driver license, national ID card, etc.) or biometric based (fingerprints, iris scans, etc.). When considering which of those options to use, some operational aspects will need to be considered but data protection as well. In some contexts, asking for ID's when a community mostly do not have such documents may not be too useful. In other contexts, the collection of biometric data may seem to be the most efficient and the only way to avoid fraud. From

a data protection standpoint, it is important to keep in mind that certain data is more sensitive than others. Whenever possible, the aim is to collect the least sensitive data.

Paper-based Identification

In many areas the easiest and common way is to ask for ID's, such as government issued national ID cards or passports. Asking for those identifiers does not pose a high risk from a data protection perspective, since those documents serve exactly for the purpose of identifying the owner. Whether it is necessary to scan or copy and file the ID's of every beneficiary is a separate question. For the purpose of identification, it is often sufficient to ask the beneficiary to present their ID to you at the registration and noting down the unique ID number. You can tick the box that identity has been checked without keeping a full copy of the ID. Alternative ID's or documents such as driver license, birth certificate, baptism certificate, electricity bills, may be accepted in lieu of a national ID if many within the communities do not have them. When collecting those documents, it is again recommended to collect as little as possible to verify the identity. More is not always better in the context of data protection. In addition, it is recommended not to ask for documentation that contains sensitive data (*e.g.*, health-related papers). Also, as discussed, it might not be necessary to keep copies of such documents.

Biometric data

Biometric data is data relating to the physiological or behavioural characteristics of a person that are recognized by technological means. Typical examples are digital fingerprints, iris scans, palm veins scans, facial and voice recognition. Such data is considered very sensitive as is highly personal and not something that could just be replaced if compromised, and therefore merit a higher level of protection. In some cases, biometric data is subject to legal restrictions including a limitation or prohibition on use. The main reason for that is the potential misuse of such data:

- **Law enforcement or security.** Biometric data can be very interesting for law enforcement or security actors, because they cannot be modified. When collecting such data in the context of a project, you might be exposed to pressure from other parties to disclose that data for other purposes.
- **Identity theft.** Biometric data is also more likely to be hacked for identity theft because they are so unique and cannot be modified.
- **Source of information in the future.** It is possible that in the future the biometric data collected today can be used to learn much more about an individual than it is possible currently. New technological solutions might be capable of reading out other information, such as genetic details.

Consequently, the collection of biometric³ data poses a high risk and should be considered as a last resort. Collection of such data must be evaluated to determine if indeed it is absolutely necessary or if an alternative solution could be used. The context of the project as well as the organization's responsibility and ability to carefully protect that data should be considered. Even when biometric data seems to be the best way to verify the identity of individuals and to avoid fraud, the potential risks for the beneficiaries must still be weighed. Especially, if it is likely that other stakeholders could claim those data for their own purposes, this risk might outweigh the practical advantages of biometric

³ For more information, please see the Handbook on Data Protection's chapter on Biometrics. As well as [ICRC's Biometrics policy](#).


data. In addition, when collecting biometric data, the considerations on safe, secure storage are even more important (see General Guidance Chapter).

Furthermore, remember the right to receive information (transparency). Such information must be presented in a way that individuals can understand it. General literacy and/or awareness of biometrics may be insufficient to allow people to understand the risks associated with this processing (it should be noted that alternatives to biometric registration should always be considered, see Project Decision 3 below).

Example:

Several geographic areas have been affected by a pandemic leading to loss in livelihoods. A cash intervention was decided for a well-developed urban community and another in a remote rural community. For registration, the heads of the affected households in the urban context were asked to bring one form of ID from a list of valid forms and documents to prove their identity. For the rural community, the head of households were requested to bring an attestation from their village leaders/heads since they lack official ID's. The beneficiaries from the rural area were then provided a temporary ID card issued by the National Society to present to the financial service provider when claiming their cash. In both cases, biometrics data collection for identification was avoided, and other means of fraud and duplication detection was used such as checking names and ages of household members and issuance of a one-time use coupon with a unique barcode that was scanned after they received their cash to indicate that they have already received their entitlement.

Project Decision 2: What other data should I collect from beneficiaries during registration?

 Data Minimization, Necessity

Project Decision reformulated: What other beneficiary data is essential for the programme?

Besides collecting data to establish identification there are other data types collected during registration for other purposes mentioned above. For such purposes, it is important to consider which data are absolutely necessary. Try to ask yourself: What do I need to use this information for and is it critical for my programme? If you are unsure or if you think you can fulfil the purpose using other data or in other ways, then consider not collecting that data. Sometimes there is a tendency to over collect because we think that data might come in handy later or because we always collect that information, or we need it for our database. The creation of a database is not an eligible reason to collect information. On the contrary, every element of personal data in that database must be there for a specific reason, for something well-defined and critical for the programme.

Using standardised templates

For registration, the use of standardised templates is very common and helpful as it speeds up data collection because commonly used data types have been identified. However, those templates tend

to cover a broad range of data because they are meant to be a “one-size-fits-all”-questionnaire. But in an emergency, these templates might be used as-is versus being analysed for data that is relevant and essential in the current programme being implemented. Collecting answers to those irrelevant questions would conflict with the principle of data minimization and necessity. This does not mean that you should not use those templates. But rather, take time to analyse and adapt the templates for each intervention. Adaptation does not mean re-creating new forms every time, but instead you may use the same form but skip the questions that are not needed (i.e., do not ask if asking questions verbally). In Excel files certain columns or rows can be hidden; on paper format templates certain sections can be redacted or scratched out; and in digital format fields could be marked not required⁴ or hidden. Team members doing the data collection will need to be informed of the data minimization principle, so they understand why certain questions are deliberately being skipped.

Examples:

In a cash programme targeting “households who lost their livelihood”. On registration day the beneficiaries are asked to fill out the standardised template issued by the National Society. The team has analysed the template in advance and has decided that households should answer all questions on the template relating to their economic situation. However, the team has scratched out all questions relating to the health condition of the family members. This information shall not be provided, because for this programme households will get the same cash assistance, whether they are healthy or ill.

The National Society is responding to a drought emergency. They also have a big blood donation programme. The team is using a standard template that includes questions related to the blood type of the beneficiaries. Since this information is not directly relevant to the drought emergency response they are working on, they decided not to ask this information from the beneficiaries and volunteers doing the data collection were informed of the reason. Alternatively, it could be explained that beneficiaries could optionally provide blood type information if they wished to participate in blood donation efforts, but that such participation would not affect any disbursement.

The following shows different purposes for collecting data and key data protection considerations:

⁴ Note a distinction here between data marked as “not required” so they do not have to be asked in case the answer to that question is needed to continue in a digital questionnaire, versus “optional” where question is still asked and it’s up to the responder whether or not to give an answer. Optional questions need to be re-considered from a data protection perspective. Firstly, information that is not needed should not be collected. Even where data is collected on a voluntary basis, the principle of data minimization applies. Secondly, optional questions still invite people to give this information and it might create the impression that they have better chances to get assistance if they tell us more. Lastly, where information is given even though it is not directly required for the project, we would have to consider whether there is a legitimate basis to process this data. It should also be recalled that it should be clearly explained to beneficiaries when “optional” information is being requested and it should be made clear that the provision of such information will not affect any assistance.

Formally verify eligibility

Although only eligible beneficiaries are invited to be registered, it could be that the verification done during the Targeting process was not formal enough or the situation may have changed making it necessary to re-verify eligibility during the registration process. Here, data related to the agreed targeting criteria will need to be collected. Considerations for this were previously discussed in the Targeting chapter. Those considerations apply during the registration process, particularly the question whether certain information would have an impact on the decision to target a person. If so, this information may be collected. Otherwise, there is no reason to do so.

In blanket distributions where there are no specified target criteria because affected people in an area are all in need of assistance, the collection of eligibility data may not be necessary unless needed to make sure they are from the affected area or establish authentication to collect assistance. The registration process in this case does not require asking about vulnerability indicators or other questions typically used to establish eligibility. Asking questions to collect typical demographic data (e.g., age, gender, household size) may also not be necessary, unless they have a relevant purpose since such data is not used to target the beneficiaries.

Effectuate cash distribution

What data is required to enable cash distribution to beneficiaries depends on the chosen distribution method. For cash in envelopes, key data to collect might be limited to basic identity and authentication information to be used during distribution. When using financial service providers (FSP), more data might be needed including Know Your Customer (KYC) data required by law for FSP's to distribute money. Details on the data collection for use by FSP's will be discussed in more detail on the next chapter. During registration, it is important to have a critical eye on what is needed and necessary to allow for cash distribution (e.g., mobile numbers to receive mobile money).

Avoid fraud and duplication

In order to avoid fraud and duplication of payments, it may be necessary to collect additional information to triangulate basic household information. For example, collecting names, ages, and gender of all household members and running a check if any of them have attempted to register as a separate household. Also, for programmes that depend on the household size to determine the amount of cash to disburse, detailed verification of households may be needed (e.g., using family cards issued by the government). In these instances, it is important to reflect on the actual context to evaluate the risk, then ensure that the data collection and processing is appropriate for the assessed risk level, rather than collecting such data in a standardized way.

Examples:

A cash programme has been set up in response to extreme heat causing fires in a small village. The target criterion (households who lost their homes) encompasses almost every household of the village. The names of the heads of those households are indicated and confirmed by the community leaders. On registration day, the heads of the households are asked to identify themselves. The team decides against the collection of data relating to family members. The risk of fraud is not very high, because most households will receive assistance and the heads of these households have been clearly identified and listed in cooperation with the community. Consequently, it is unlikely that other family members or people from other villages can falsely claim assistance.

A cash programme has been set up in response to food insecurity in a small community targeting women-headed households. The cash grant is relative to the size of the household to meet their needs. The programme team decides to collect the household size because it is necessary for the grant calculation, but it is most likely not necessary to collect additional information on the individual family members. Since the community is small it is unlikely that people will try to indicate higher figures for their household size because other community members will likely know and report the discrepancy.

The same cash programme has been rolled out in larger, more dispersed communities. The cash grants are higher due to cost-of-living adjustments. There were some reports of overinflating household sizes in previous programmes run by other NGO's. The programme team's analysis indicated high risk of potential fraud and decides to collect additional information about the family members (name, age, gender, degree of kinship or affiliation to household). Additional data was used to cross check duplicates in the registered beneficiaries list.

Note: For programmes that use self-targeting or self-registration, where beneficiaries apply based on published target criteria, it is important to note that data is collected also for those that do not meet eligibility. It is recommended to ensure that when it is obvious that the individual is not eligible, his or her data be deleted or archived to prevent re-registration attempts (as necessary). If further verification is necessary, then store the data for a limited time until the verification process is done and if not eligible, inform the applicant and delete their data accordingly. See General Considerations chapter for data storage of non-beneficiaries. Also, make sure published target criteria are narrow and detailed to limit number of non-eligible applicants.

Project Decision 3: What should I tell beneficiaries about the handling of their data?

 Transparency

Project Decision reformulated: How can I make sure beneficiaries have access to information relating to the handling of their data?

The data protection principle of Transparency means that beneficiaries as data subjects must receive clear communication on why their data are being collected and how their data are handled. This encompasses the purpose of the collection, the storage, potential data sharing, the rights of the beneficiaries, etc. To inform the beneficiary about all of this may be challenging in some situations, particularly in emergencies where time is limited. Furthermore, where beneficiaries have urgent and more pressing needs than data protection, they may not be as interested in hearing about those details or understanding what they mean. Nevertheless, they have a right to this information.

A good approach is to give the beneficiaries some **basic information** and a **contact** to go to if they want to learn more. This should be included in the Community Engagement and Accountability (CEA) plan for the programme (see Module M4_2 of the CiE toolkit). Basic information could be provided during the meeting with the communities to explain the programme and could be re-iterated during

the beneficiary registration process. A general privacy notice could also be prepared, printed, and shared by the National Society along with details of the programme (see Privacy Notice template in the reference section). Beneficiaries can consult this notice and if necessary, contact the National Society for more information when they need it. The key is for beneficiaries to be able to reach someone either via a hotline for those with access to phones or in person.

When providing information about data handling, it is helpful to put yourself in the beneficiaries' shoes and ask yourself: What information do I need to know before providing my personal data? Common basic information is listed below. This information should be presented clearly, in an easy-to-understand manner, and in the appropriate language(s).


- **Purpose of the data collection on registration day.** Refer to the purposes set by your programme—some common purposes discussed above include the need to prove their identity, verifying eligibility, effectuating cash distribution, or avoiding fraud and duplication. Beneficiaries need to know about those reasons and why certain data are needed for these purposes; it helps them understand what is going on.
- **If you have collected data about them from others** (e.g., other NGO's, community leaders, government). Very often you receive information about beneficiaries from other sources before you contact them directly. It is important for beneficiaries to learn where you got their personal information from, so they can feel confident that their data is being used responsibly.
- **How to have inaccurate data corrected.** For beneficiaries it is reassuring to know that they can correct inaccurate data anytime. Mistakes happen particularly when actions are rushed during an emergency, both from the programme team doing the data collection and from the beneficiary providing initial data. If the information is found to be wrong, the beneficiary should be able to request correction.
- **How to express concerns or file complaints.** Beneficiaries should know that they can express their concerns about the handling of their data. This is important for them to know since it gives them a sense of control. They may want to object to the data processing or complain about it. If that is the case, they should know where to go and with whom they can talk about their concerns and their options. This should be part of the feedback and complaint mechanism for the programme (see Module M4_2_5 of the CiE toolkit).
- **Intention to share data.** If you know that you will share the data collected with other groups or institutions (e.g., other NGO's, FSP, government), the beneficiary should know about it and why there is a need to share their data. After all, the beneficiary gives this information only to you and trusts you to keep it safe. In some contexts, the beneficiary may not want certain types of information to be shared with other entities due to sensitivity or safety concerns. It may help to do a due diligence on such institutions so you can communicate their reliability in terms of handling of beneficiary data. Furthermore, if beneficiaries detect potential misuse of their information because they were shared with external entities, they should be encouraged to inform the National Society via the helpdesk or direct contact for such matters.

In addition to the basic information mentioned above, it would be good to ensure additional details about data handling are prepared in case further questions from the beneficiaries arise. Other information the beneficiaries should receive (depending on the context) includes:

- How their data is stored and security measures
- Retention period envisaged for the data
- Legitimate basis on which the processing is based
- Any additional information on purpose or further processing
- Any additional information on data sharing

- Other Data Subject Rights that may apply, such as right to erasure, to object, and to access their data

Project Decision 4: Should I ask beneficiaries for consent?

 Legitimate Basis

Project Decision reformulated: What legitimate basis should I rely on?

The question whether you should ask a beneficiary to consent to the collection and use of their data has many layers. It has become common practice to start beneficiary registration forms with a question on consent before proceeding. At first glance, it sounds right to do this—it is polite and respectful to get permission. However, under data protection law the processing of personal data can be based on other grounds than only consent, which will be discussed in more detail below.

But wouldn't it still better to ask for consent? Not necessarily. It might seem like a sign of respect to ask the beneficiary to agree, but it comes with some challenges to consider.

Problems with consent

Consent needs to be freely given and fully informed. In practice, this means that consent is only valid when there is a real option to refuse, otherwise it is not truly “freely given”. In case of emergencies, obtaining consent may not be feasible. Beneficiaries are in a vulnerable and desperate situation in need of immediate help. Data protection might not be their first concern. Hence, they might provide “consent”⁵ because they see no other option to get support. And indeed, without their data you cannot help them.

Also, beneficiaries might not be in a position to fully comprehend the consequences of them providing their data or how their data is processed (e.g., via technology). You cannot meaningfully agree to what you do not understand (so it cannot be considered as “fully informed”).

One other issue to be aware of is that consent can be withdrawn at any time and without cause (if it is freely given, it can be freely taken). Once consent is revoked any further processing of the concerned personal data (that was done on the basis of consent) is forbidden. This can become very problematic for the programme, because it is important to have a reliable set of data to work with. After consent has been revoked, it may no longer possible to go back and use another legitimate basis, such as vital interest or public interest. Why? Because their right to withdraw is worthless if afterwards nothing changes for them, and it also depends on whether another legitimate basis can be identified and what information was already provided to the beneficiary. For all those reasons, consent can be problematic to use as a legitimate basis. For the processing of personal data in the context of cash programmes in emergencies, it is recommended to consider other options.

⁵ Consent is in quotation marks because while the beneficiary may check a box or make some other indication that they consent, it would not be correct to say that it would be legally recognized as consent under general data protection laws and principles.

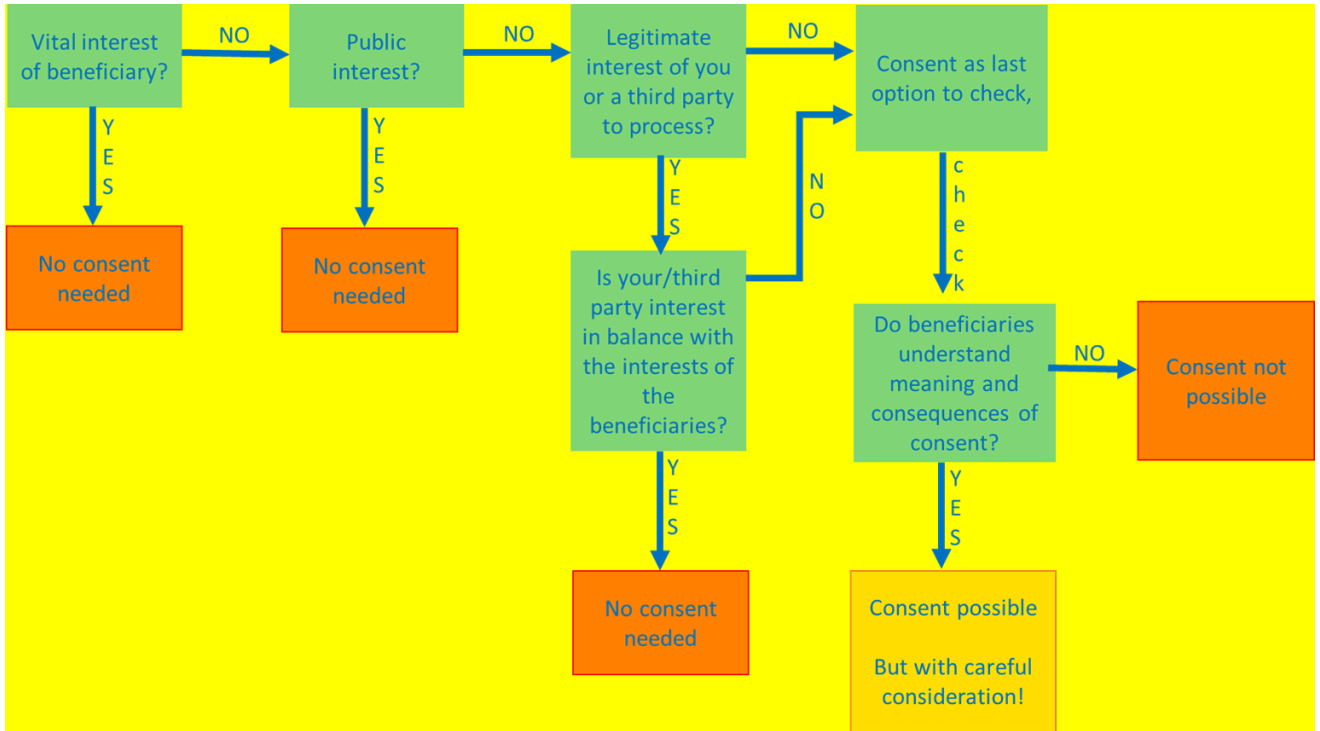


Figure 3: Decision tree for determining whether Consent is an appropriate legitimate basis

Other options

Figure 3 shows other options for establishing a legitimate basis. Two of those options are vital interest and public interest. **Vital interest** means that the processing of personal data is essential for the beneficiaries’ life, integrity, health, dignity, or security. CVA programmes designed to address lifesaving or essential needs at the onset of an emergency may qualify for this; for other CVA activities in non-emergency context may need to look at other options. **Public interest** means that the processing of personal data serves a purpose that is in the interest of everybody. National Societies providing assistance fulfil a humanitarian mandate which is in the general public interest. Hence, even where the high standard of vital interest is not fulfilled, assistance through CVA will normally still be in the public interest⁶.

To avoid misunderstanding: It is still the beneficiaries’ choice if they want to participate in the programme or not. But if they decide to do so, it is okay to use their personal data without explicitly asking for consent to do so provided they are informed about the programme and how their data will be used. It is in their vital interest and/or in the public interest. What is important, is that you only use personal data that is absolutely necessary for the programme. See also the Cash Transfer Programming section of the Handbook on Data Protection for more details on legal bases for CVA.

Data sharing

Data sharing with other entities (e.g., other NGO’s, government, FSP) can be in the vital interest of the beneficiaries or in the public interest. Additionally, there may be legal obligations to share certain

⁶ Please note that in some jurisdictions relying on public interest might require additional considerations or an official government approval. It is beyond the scope of this guidance to verify this for every jurisdiction. If you have doubts whether you can rely on public interest for your programme, please do not hesitate to communicate to your manager or the legal team of your National Society.

personal data⁷ and if so, this can be done without consent. Where no legal obligation exists, it can be in the legitimate interest of your National Society to share personal data. Your legitimate interest can justify data sharing without consent if the beneficiaries have no overriding, opposing interest. It is crucial to consider the potential consequences or risks for beneficiaries if data is shared. This is explained in more detail in the Chapter on Data Sharing. In short, it all comes down to necessity and confidentiality.

Programme administration

Certain project decisions relating to the handling of data may not be directly in the vital or public interest but are still reasonable from a programme's perspective (e.g., kind of storage, inclusion of more team members, etc.). Here again, the legitimate interest of your National Society to structure and organise the programme in an effective and efficient way comes into play.

So?

In most cases it is not necessary to collect consent. That does not mean that your actions are less justified – on the contrary. However, there are two more points to consider:

- Not asking for consent does not mean that you do not have to **inform beneficiaries!** Regardless of the legitimate basis you want to use, the principle of Transparency applies. As described in Project Decision 3, some basic information regarding the handling of the personal data and a contact for further questions are good standards.
- You may consider changing your consent question to “do you have any questions or concerns before we proceed?” or “do you acknowledge receiving basic information about the programme including where to ask for more details about how your data will be used?” This is not compulsory but could be an alternative way of being polite and respectful before asking for more personal details.
- Do you have to evaluate the legitimate basis for every CVA intervention you do? Not necessarily. Most CVA interventions may cover the same legitimate basis, just remember not to use Consent as the default. If the nature of a new CVA programme is unique and impacts to beneficiary data are not clear, then it would be good to formally assess the legitimate basis before proceeding. It is also advisable to conduct a Data Protection Impact Assessment (DPIA) in this case. See General Guidance Chapter for more details on this.

V. Use of Financial Service Providers

Personal Data Use

Distribution of cash and voucher assistance is usually done with the support of service providers and therefore a contract is established with them. For voucher programmes, providers include commodity merchants, local vendors, supermarkets, and wholesalers. For cash programmes, they are financial service providers (FSP) such as banks, mobile network operators, or remittance agents supporting encashment. For this chapter, we will focus on FSP's but note that the data protection principles should be considered for all types of service providers. Use of service providers can be reviewed in Module M4_3 of the CiE toolkit.

⁷ Please note that compliance with a legal obligation is a generally recognized legitimate basis under many data protection laws.

Data Protection Considerations

The use of FSP's may require sharing personal data of beneficiaries to be able to distribute cash. This section will look at key project decisions when working with FSP's and the considerations related to data protection. Risks related to data protection and FSP's should be included in your programme's CVA Risk Matrix developed from your programme's Assessment and Response Analysis phases. See Module M2_4_3 Assessment and Module M3_1_4 Response Analysis in the CiE toolkit.

Project Decision 1: Should I use a Financial Service Provider?

 Data Minimization, Necessity and Data Security

Project Decision reformulated: Could the FSP use the beneficiary data in a way that would be detrimental to the beneficiaries?

When considering whether you should use an FSP in your project, it is important to analyse what data will be required by the FSP to provide their service, which may involve asking additional information from the beneficiaries for this purpose, and carefully evaluate the potential consequences for the beneficiaries when such data is shared.⁸

Know Your Customer (KYC) and Watch List Screening

Many FSP's are subject to KYC regulation, which requires them to collect information about their customers to prevent money laundering, terrorism financing, or other crimes. The amount of information required could depend on local regulations with some countries allowing greater flexibility based on what they see as the level of risk with the transactions. Humanitarian agencies using FSP's will need to comply with such KYC regulations requiring to share some data from beneficiaries.

Some considerations to ensure the principle of minimization and necessity is observed:

- Investigate the KYC regulations in your country and operating context. Determine what data is required by law and cross check that against what the FSP is requesting. There might be internal policies for why FSP's are asking for additional data outside of what is required by law; this needs to be justified and negotiated to ensure only what is strictly necessary to provide assistance is shared.
- In certain cases, humanitarian organizations could advocate for simplified or adjusted KYC requirements (e.g., reducing requirements for people that have lost their ID's, capping amounts that could be transferred to beneficiaries or tiers for KYC, or allowing for cash transfers for a limited time). Check if in these cases data shared with FSP's could be minimized.
- Inform beneficiaries and explain the KYC requirements or at minimum include these requirements in the privacy notice that could be consulted at any time.

FSP's may have obligations to check KYC information and share data with third parties (such as regulators and public authorities). Such KYC checks may include running the list of beneficiaries against watchlists, sanctions list, or lists of designated persons by local authorities that might be involved in conflict or violence. Some FSP's do it systematically while others on request of the government. This

⁸ A questionnaire template for FSP can be found in the reference section of this guidance.

process will flag individuals that might be suspected to be involved in certain criminal activities (money laundering, terrorism, corruption, etc.) and therefore not eligible to receive cash. If a beneficiary's name is a match on one of such lists this can have severe consequences for them. It is therefore crucial to analyse the country and programme context. Typical questions to think about are:

- Are there reports of political or ethnic, or religious persecution by the government?
- Are parts of the beneficiary population considered as opponents of the regime?
- Could political parties be considered as terrorist groups?
- Is the FSP closely linked with the state authorities, such as intelligence services or security agencies?
- If beneficiaries are refugees, does the FSP have a branch or storage facility in the country of origin of the refugees where data might be requested by authorities?
- Would there be serious concerns or fear from the beneficiaries if their data was somehow shared with the government due to these obligations?

If you suspect that beneficiary data might be used in this inappropriately, this presents a severe risk for beneficiaries. Under these circumstances, if you cannot find a way to contract an FSP without sharing beneficiary data, other distribution options, such as cash in envelopes, vouchers, or even in-kind, should be considered. This should be done as part of Risk assessment during the Response & Analysis phase of your programme (Module 3 of the CiE toolkit) and should include an analysis whether persecution, exclusion, or other sensitivities could result in collecting and sharing KYC information in the selection of the best transfer modality. Other references from CaLP: [Know Your Customer Standards and Privacy Recommendations for Cash Transfers](#) and [KYC Regulations Tip Sheet](#).

Other purposes


Given that FSP's are typically for-profit companies they might use the beneficiary data for their own purposes including commercial interests, such as profiling for credit worthiness, advertising or marketing, and checking for eligibility for other financial services. Such examples may seem relatively low risk to the beneficiaries but are still considered outside the purpose of humanitarian cash assistance. Data protection law is also meant to protect people from private institution's unsolicited actions such as spamming.

Other potentially higher impact of FSP's reuse of data could be for offsetting debt (e.g., beneficiary owes a loan or money from the bank and the bank tries to deduct their cash assistance to pay off what was owed) or further sharing of data to third parties such as debt collectors.

In general, due diligence on the reputation and performance of FSP's should be done during the tendering or contracting process.⁹ Also, contracts with FSP's should restrict further processing of data (during and even after the cash distribution), and include examples of actions that should be avoided, if those are known at the time of contracting (see Project Decision 3). During programme implementation, beneficiaries should be asked/requested to report to the National Society any instances of further use (or suspected misuse) of their data by FSP's that are outside of the programme.

⁹ A questionnaire template for FSP can be found in the reference section of this guidance.

Project Decision 2: Which account type should I choose for the cash distribution?

 Data Minimization, Necessity and Data Security

Project Decision reformulated: Which account type to use for the cash distribution best protects the data of the beneficiaries?

There are different cash payment mechanisms to consider including the use of banks, remittance agencies, mobile network providers, and post offices. From a data protection perspective, it is important to consider, regardless of which payment mechanism option is selected, how to limit the sharing of personal data. And this could basically depend on type of account used for the cash distribution. Consider two types of accounts: using named accounts for individual beneficiaries or having a virtual account managed by the National Society.

Named accounts

The programme may choose to directly use the beneficiary's account with the financial service provider or open an account on their behalf. Using pre-existing beneficiary accounts interferes less with data protection than opening new accounts because the FSP and the beneficiary already have a contractual relationship which your National Society leverages for the purposes of the programme. The creation of new accounts by the National Society for individual beneficiaries, assuming this is feasible, should be analysed in more detail to determine possible data protection risks. For instance, there might be a specific reason why the beneficiary has not opened their own individual account (e.g., due to some KYC concerns mentioned in the previous section). Opening an account on behalf of another person requires care in the collection and sharing of data with the FSP, as well as managing such account after the programme.

Virtual accounts

Virtual accounts are owned and managed by the humanitarian organization where they could create sub-accounts for beneficiaries to allow them to receive cash. With such accounts, the KYC is done with the organization and not the individual beneficiaries. Examples of use of virtual accounts:

- Issuing of prepaid ATM cards where each card is linked to the National Society's account and given to eligible individuals with a PIN that could be used to withdraw cash
- Issuing bank checks to individuals that could be redeemed regardless if they have an account in that bank
- Limited use mobile SIM issued by the organization so beneficiaries can receive an SMS with transactional codes that could be used to redeem cash from mobile money agents

Beneficiary data may still need to be shared with the FSP for identification purposes at the time of cash disbursement, but the amount of data to share with the FSP is generally reduced compared to creating named accounts because KYC is not being established with the individuals. From a data protection standpoint this option is attractive, but there are some operational considerations too (e.g., capacity of the programme team to manage the sub-accounts, distribution of tokens such as prepaid cards to collect cash to the right individuals and linking the right sub-account numbers, and reconciliation of transactions post disbursement). The risk of managing transactions and funds are mostly with the agency. Also, when using virtual accounts, the NS has access to data revealing how beneficiaries use their cash. This data is sensitive. In order to respect the beneficiaries' privacy in this

respect, refer to the chapter on Post-Distribution Monitoring for more details on privacy and monitoring.

Project Decision 3: What should the contract with an FSP contain?

 Data Security

Project Decision reformulated: What provisions should I include in a contract with the FSP to protect the beneficiaries' personal data?

Firstly, it is important to determine what data is absolutely necessary to fulfil the FSP's service and negotiate to minimize data sharing. This would typically include:

- Identification data such as beneficiary name and valid ID number
- KYC required data which could vary based on national regulations
- And other data, if applicable, required to enable the cash distribution such as: mobile phone number for mobile money transfer, bank account number, or name and ID of the person who is authorized to receive cash on the beneficiary's behalf (proxy)

It is also important to understand what data might be created by the FSP and shared with you as part of the transactions done with the beneficiaries. For example, date and status of encashment, signature of beneficiary after receiving cash, current balance if not all of the cash has been withdrawn from the account yet, where cash might have been used (e.g., grocery store), etc.

Secondly, a contract or service agreement will need to be created. This agreement should include the framework for the service provision, scope, and data protection elements. It is recommended to have a template for this agreement prepared and shared as part of the tendering process, and data protection considerations evaluated as part of the selection of the vendor.

Some of the key provisions to include in the contract:

- **Purpose limitation.** Data shared shall only be used for the purpose of the programme (cash distribution). Any other further use outside of the scope of the programme shall not be allowed. As mentioned above, it may also help to be explicit or list concretely the examples of what the data should not be used for (e.g., advertising and marketing, offsetting debt). List should be marked "non-exhaustive".
- **Data sharing with others.** The FSP shall not share the data with others if this is not approved by the National Society. Also, in the event of an obligation to share (e.g., with authorities), that the National Society should be informed first.
- **Data security.** Data shared shall be stored safely (e.g., indicate access controls, encryption, backup processes).
- **Confidentiality.** Data shared shall be treated confidentially.
- **No additional data collection from beneficiary.** FSP shouldn't collect further personal data from beneficiary under the umbrella of the programme. E.g., beneficiaries may need to show their ID's for identification when claiming cash assistance, but the FSP should not copy or scan the ID and thereby collect additional data of the beneficiary.
- **Deletion.** Data shared shall be deleted from FSP databases upon completion of the programme or archived offline and securely for audit purposes.
- **Consequences of a breach by the FSP.** The contract should contain language stating that the FSP acknowledges that a breach of these terms may have legal consequences,



but at the very least cause reputational damage to all parties involved. Indicate that beneficiaries are encouraged to inform the National Society of any non-programme related use of their personal data by the FSP.

Please see the references section below for sample template from the IFRC in contracting with FSP's. It contains the relevant points on data protection. If you feel like something is missing or want to address a specific issue that has come up in the context of your program, you can add these aspects in your own template.

In practice, the FSP often wants to use their own contract template. Depending on your bargaining position, try to negotiate using your National Society's prepared template. If you do go with the FSP's template, it is advisable to take a closer look and compare the data protection elements and request for them to be amended to ensure strong protection of your beneficiaries' data. If the FSP's template does not contain any language on data protection, this is your chance to introduce the data protection aspects you think are important. You can extract certain clauses of the IFRC template. If the FSP does not want to accept any language on data protection in the contract, this should be a red flag in terms of working with this vendor. Every reputable entity should be interested in a minimum data protection standard.

It is typical to negotiate a framework agreement with one or several FSP's as part of cash preparedness so you may have options depending on context and needs. However, new programmes may come into new situations that are not part of the current agreement with the FSP. If you have the impression that data protection has not sufficiently been addressed in the framework contract, do not hesitate to communicate this to the FSP or to your manager to try to negotiate an amendment. Data protection has become more and more important over the last years and awareness is only beginning right now.

VI. Data Sharing with Government, other Humanitarian Organizations, and Donors

Personal Data Use

CVA interventions require cooperation and coordination with wider stakeholders such as national government, other humanitarian organizations (international and domestic), and donors. In these relationships it is possible that the beneficiary data of a National Society might need to be shared externally (and the National Society may also receive data). Sharing might be formally done via data sharing agreements or informally with no set agreements, particularly in emergencies where timeliness is key.

In the Targeting chapter we saw examples of receiving beneficiary data from the government and other organizations responding to the same emergency to establish a preliminary beneficiary list and to verify eligibility of those in the list. This level of data sharing is also important for coordination between the various actors to avoid costly duplication of efforts and assistance. For donors, there could be some obligations to audit and demonstrate transparency and accountability by ensuring the beneficiaries that have received assistance are real people, were indeed eligible, and that they did receive their cash entitlements.

Data Protection Considerations

In this section we will look at key data protection considerations when sharing data with external parties. In general, when sharing data with different parties, **it is important to ensure data is safely transferred via secured means** (e.g., encrypted files, stored in secured data rooms) and accessed by authorized personnel only. See General Guidance Chapter.

Where data is transferred to other countries it is key to evaluate the level of data protection in this country. If it is lower than the NS standard, the transfer should be reconsidered and if inevitable, a solid and detailed data sharing agreement on data protection requirements should be negotiated.

Project Decision 1: Which data should I share with government?

 Data Security and Necessity

Project Decision reformulated: Is it necessary and safe to share personal data with the government?

National Societies, though acting as auxiliaries to their country's government, have a duty to uphold their neutral, impartial, and independent nature when it comes to humanitarian action. Yet, they are also subject to national laws¹⁰ where there could be legal obligations and therefore mandatory to share certain data with the government. Some of the data protection risks were discussed in the KYC section (related to the use of FSPs) in terms of reporting designated persons to the authorities (watchlists, sanction lists). There could also be risks of the National Society getting pressured by authorities to share personal data for other purposes (e.g., combat terrorism). Hence, an analysis is needed when designing the CVA intervention—way before collecting data—and document these risks (using a Risk matrix or a more structured analysis using a DPIA).

Besides the specific national laws, there are other purposes for which data maybe required by the government from the organization:

- **Gain understanding of the CVA intervention.** The government often wants to be informed about humanitarian programmes organized in their jurisdiction as they are ultimately responsible for the safety and well-being of citizens and inhabitants in their areas. Additionally, if there are disagreements between some community members on why they are not included in the programme they bring their complaints to the authorities. Typically, authorities would like to understand the purpose, duration, target groups and agreed targeting criteria, financial scale, security requirements, resources and support needed from them. For the government to develop an understanding of the programme, it is normally sufficient to provide general information and aggregated data (target criteria, areas, number of people supported, percentage of elderly/children, amount of cash grant, etc.). In some cases, they might be interested in seeing the final list of beneficiaries that have been targeted. If this list is not already made public through community communication and sensitization, it is good to understand why the authorities may need such a list and negotiation may be required to limit any personal data provided.
- **Coordination to avoid duplication of assistance.** In an emergency, the government normally have programmes to support affected communities, as well. If there are different agencies providing assistance, the government units may take on the coordination to ensure there is no duplication of assistance and support agencies to deliver aid as quickly as possible. In some countries and contexts, the government may request beneficiary data from all organizations to check for duplication, and in some cases may even need to validate the list before the organization could proceed with the distribution. The intention to avoid duplication can be reasonable and requires the government to learn about the beneficiaries' names. Other personal data, though, is not necessary to be shared for this purpose. Also, there is generally no need to give the

¹⁰ Exception are those with privileges and immunities.

government access to your database. Where possible, negotiate to minimize data to share with authorities to facilitate coordination and duplication checks.

- **Implementation partnership.** The National Society could be in a partnership with the government to distribute on behalf of the government. Social protection programmes and large distributions where the government may rely on the National Society's reach and capacity. In such partnerships, a formal agreement is typically created. When negotiating such agreements, please keep in mind the data protection principles and best-practices.

No matter the official purpose, two potential issues are to be kept in mind. Firstly, in certain contexts, it is conceivable that personal data once they are shared, could be reused for other purposes. Secondly, even where you only share a very limited amount of personal data, these data can possibly be combined with other data that the government already holds. The consequences this might have for beneficiaries, are hard to predict. To limit those two risks, it can be an option to only present a hard copy of the beneficiary list. Non-digitalized data is more difficult to reuse. Even better is to only show the list in a meeting and to take the hard copy back with you right away. It depends on the context whether the government will accept such an approach, but the idea here is to try options to minimize data sharing.

Where personal data must be provided to the government, remember:

- Be clear on the purpose for sharing the data and the potential consequences or risks to the beneficiaries; mitigate where possible and identify a legitimate basis.
- Establish a data sharing agreement, if feasible. Such agreement will formally outline the purpose for which personal data is shared and will limit the usage of the data to this very purpose. It also requires the recipient to keep the personal data safe and stored for no longer than necessary. Refer to the IFRC FSP template¹¹ for general guidance. The National Society has an auxiliary role to the government, which could be important in negotiating data sharing agreements.
- Inform the beneficiaries that data will be shared with the government and explain why. Be clear also which government units the data will be primarily shared with. This may deter certain beneficiaries from sharing their data and should be addressed by the programme.

Project Decision 2: Which data should I share with other NGO's?

 Data Minimization, Necessity and Data Security

Project Decision reformulated: Is it necessary to share personal data with the other NGOs and can it be done safely/securely?

Sharing information with other NGOs might be necessary in certain contexts. The following are some examples and key considerations for data protection should include the following questions:

- Is it in the interest of the beneficiaries to share their data?
- Would it expose the beneficiaries to a risk?
- Can I make sure that the data is kept confidential and will not be shared with others without my approval?

¹¹ The template of a contract with FSP can be found in the reference section of this guidance.

- Does the other organization have sufficient data protection standards?

In any event, sharing more than names and contact details will be problematic. Vulnerability indicators tend to be very private and, when possible, the beneficiaries should themselves have the possibility to decide with whom they want to share these data.

For coordination. Sharing data plays a role where several humanitarian actors are simultaneously providing CVA assistance and it is necessary to work in coordinated fashion (e.g., local cash working groups). With different programmes running at the same time, it is important to avoid duplication and make sure that harm is not done because of the actions of the various actors. Some coordination efforts look to harmonize cash grant amounts, targeting criteria, and approaches. Despite these reasonable intentions, it is advisable to keep a critical eye and to consider whether it is really necessary to share personal data – and to what extent- in order to coordinate work. Often it is a good alternative to share general information and aggregated data (target criteria, geographic areas targeted, number of people supported, percentage of elderly or children, amount of cash grant, etc.). Even where the purpose is to avoid duplication, it is not automatically necessary to compare beneficiary lists. Depending on the context, duplication may be avoided by allocating different areas of activity (village A/village B) or different target groups (pregnant women/elderly). Where you conclude that sharing of beneficiary data is inevitable, data protection demands you to limit the amount of data shared to a minimum. For example, it might be sufficient to compare beneficiary lists on paper in a common meeting with the other NGOs. This is less of a risk than giving other NGOs access to your database or sending lists via email.

Leveraging expertise and reach within a community. In certain situations, one NGO might have specialized knowledge of a sector or groups within a community (e.g., groups targeting vulnerable women and children). Here a National Society may need to cooperate with such NGO to benefit from their expertise or knowledge of the community. Many times, other NGOs rely on the local National Society because of their grassroots presence in many communities and at times the only humanitarian actor present there.

There might also be situations where another NGO wants to set up their own project based on your pre-existing beneficiary dataset. This is practical and saves time in data collection. However, this means further use of personal data which may not be compatible with the original purpose of data collection. Even if this seems more convenient from beneficiaries' perspective because they may receive more assistance, data sharing here is still an exception, not the rule, and it is advisable to be cautious.

Implementation partnership. Data sharing is also important in implementation partnerships where one organization might be contracted to deliver aid/services on behalf of another organization or to share responsibilities in the CVA implementation. E.g., the UN refugee agency working with several NGOs providing services to refugees. In such partnerships, data sharing is normally negotiated and included in a contract or agreement. In conducting such negotiations, it is important to evaluate risks to the beneficiaries when data is shared and handled by partners, as well as roles and responsibilities of the partners and the shared responsibilities to data protection. It is possible that the lead agency may dictate the data protection standards, however if your evaluation of risks finds gaps or if you think certain provisions need to be strengthened, do not hesitate to communicate these with your manager and/or discuss with the legal team within your National Society so they may be addressed in the negotiation process. For instance, if your National Society collects data from beneficiaries, do you need to turn over all that data to the lead partner or can you minimize data to what is essential to fulfilling your responsibilities in the partnership? If you have parallel CVA programmes targeting the

same beneficiaries under the implementation partnership agreement, how do you ensure separation of access from partners for things outside the scope of the agreement?

Common platform. There are some initiatives to develop a common platform in terms of sharing beneficiary data and potentially using the same payment mechanism by several participating organizations. This may involve having one database or a mechanism to have interoperability of data systems owned by the agencies to share and expose the agreed set of beneficiary data. Such a platform aims to improve coordination and collaboration among humanitarian actors and may be endorsed by some donors as it may improve efficiencies. There are different approaches for having such common platforms and the National Society should again evaluate the needs and risks for the beneficiaries ahead of efficiency gains of the organizations. Some questions to consider:

- Is such a platform absolutely necessary for the National Society to deliver cash assistance? There are different ways to coordinate and collaborate with other NGO's that may not require direct access to beneficiary data.
- What data is required to participate in the common platform and can they be minimized?
- How should the beneficiaries be informed when their data is used by other agencies? And who should inform them?
- Once the data is shared via the common platform (i.e., the other agencies have access to your data) how do the partners ensure the data is used for the agreed purpose(s)?
- What are the security features of the platform to ensure only authorized personnel can access the data?
- What would be the governance for data access by the different NGO's? The more NGO's join it typically becomes more challenging to manage. Particularly when one organization decides to stop participating in the common platform, how would the data they share be used going forward?
- Where will the data be stored and does that location (for instance, outside of the target country) raise data protection compliance issues?

If the decision is to share personal data with other NGOs, firstly, it is important to have an agreement in place. The legitimate basis for the processing should be identified. Where data sharing will be done via a common platform, this agreement must be even more solid, with robust data protection standards, scope, and roles and responsibilities of the participating partners defined. It is recommended to involve IT-experts and legal experts in the negotiation of the agreement for a common platform to ensure a sufficient level of protection. Secondly, beneficiaries should be informed that data will be shared with other agencies. If data sharing was not intended at the time of the collection or registration, it will be difficult for you to inform every individual. In this case, it should be the responsibility of the other NGO using the data you shared to inform those beneficiaries. It is advisable to make this clear in the data sharing agreement.

Project Decision 3: Which data should I share with donors?

 Data Minimization, Necessity and Data Security

Project Decision reformulated: Is it necessary and safe to share personal data with the donors?

For donors it is important to ensure accountability and transparency in their funding activities and therefore may ask you to share some beneficiary data. It is again important to think about potential risks for the beneficiaries' privacy and to consider options to limit the amount of data shared.

There are two main purposes for donors to request and use beneficiary data:

- **To gain understanding of the programme and monitor status.** The donor typically wants to understand the circumstances in the field and how the programme team is responding. Here, it is normally sufficient to provide general information and aggregated data (target criteria, areas, number of people supported, percentage of elderly/children, amount of cash grant, etc.). Sharing details of the names and other personal data is not usually necessary. The donor might also be interested to learn how the beneficiaries spend the money they receive.¹² Again, aggregated data should suffice (e.g., percentage of people who spent money on food and other commodities, percentage of people who kept the money longer than a week, etc.).
- **To fulfil audit requirements.** The donor often requires beneficiary data to fulfil its audit requirements. Donors must make sure that money donated actually is used for the intended purpose. Other audits check if the beneficiaries are real people, that they met the agreed targeting criteria, and that they actually received the cash assistance (proof of receipt). For these audit related activities, there are different options to protect the privacy of beneficiaries privacy protecting options:

When **sharing a list** to conduct the checks the data included could be limited to the required minimum, and potentially instead of exposing beneficiary names, unique reference ID's could be used. . For proof of receipt for instance, the name, the date and the signature showing they have received cash should be sufficient. In some cases, even the name may not be necessary as long as the beneficiary ID is provided. If the signatures were collected on paper which contain more information than necessary, the respective columns should be redacted, removed, or blacked out before sending them to the donor to increase data protection.

Another approach is to **give limited-time, read-only access** to the database or documentation where auditors can do their spot checks. The donor's auditors can verify the relevant data or documentation in person together with you, without downloading or taking any data with them. You can discuss with the donor in advance which information is necessary and the methods to do these checks. Data sharing with donors should be included in the contract or agreement with them.¹³ Legitimate basis

¹² Please note that this sort of information should not automatically be collected. There must be a legitimate reason for collecting information about the purchases made by beneficiaries. Before collecting such information, which may reveal sensitive information about the beneficiaries, undertake a data protection review. See Post-Monitoring Chapter.

¹³ It is important to consider issues such as audit requirements at the contract negotiation stage.

should be identified and beneficiaries should be informed about the intended data sharing with donors.

VII. Post-Distribution Monitoring

Personal Data Use

To understand whether the CVA programme objectives are being met, a monitoring and evaluation strategy is needed. Part of this strategy is to determine the indicators necessary to identify outputs, outcomes, and impact, as well as the methodology for getting and analysing such indicators. There are various types of monitoring including market monitoring, baseline monitoring, encashment monitoring (typically using exit surveys), and post-distribution monitoring. For this section we will focus on post-distribution monitoring (PDM). For more details on monitoring and evaluation, see Module M5_2 Programme Monitoring of the CiE toolkit.

For humanitarian organizations and donors, it is important to know how and when beneficiaries use the money they received. PDM's are usually conducted a few weeks after a cash distribution to allow for the beneficiaries to use the money they received. PDM's are useful to evaluate the quality of the programme and to improve future cash programmes and most likely use personal data. Depending on the programme there could be multiple visits to the beneficiaries to monitor progress (e.g., shelter construction as part of recovery) where different datasets will have to be tracked over time.

Data Protection Considerations

The word "monitoring" might indicate that beneficiaries are being controlled in a certain way, their behaviour analysed. But actually, it is not the beneficiary, but the programme and its effectiveness that is monitored. . However, that does not mean that monitoring (of the programme) will not have a consequence for the beneficiary. Thus, beneficiaries' privacy must be considered.

Please note: The Project Decisions of this chapter will focus on PDM. For baseline and encashment monitoring the key aspect is data minimization/necessity. When collecting data from beneficiaries, it is important to think about which data is really necessary in the context of monitoring your programme. When using standardized templates, they need to be adapted to the context by redacting unnecessary questions. Refer back to the chapters on Targeting and Beneficiary Registration. Another recommended method to increase the level of data protection in baseline and encashment monitoring is to remove direct identification of the beneficiaries (e.g., names and personal ID's).

Project Decision 1: What personal data should I collect in the monitoring process?

 Data Minimization, Necessity

Project Decision reformulated: How can I limit the use of personal data in the monitoring process?

Depending on the context, monitoring can be done in different ways. Here we will look at PDM for conditional and unconditional transfers and the data protection considerations.

Conditionality and Restriction

The CVA programme may have certain *conditionality* (prerequisite that beneficiaries need to meet before receiving cash such as attend school, health promotion, livelihoods workshop) or *restrictions* (requires beneficiaries to use assistance for specific items or services or achieve an output such as

repair shelter or start livelihoods). The purpose of monitoring is to verify whether conditions remain fulfilled and restrictions are being respected over time. A key consideration is the privacy of the beneficiaries. This can be done by reducing the amount of information collected to what is absolutely necessary. Additionally, it is helpful to set reasonable time intervals for the monitoring and to limit the number of persons involved in the monitoring of the same beneficiaries. Also, limit access to disaggregated data that might be used by different stakeholders assisting or involved in the monitoring process.

Example:

In the context of a programme, beneficiaries are to use their assistance to build shelter after a devastating hurricane. The programme team decides that they will visit each beneficiary after one week and again after three weeks to see how the shelter reconstruction is progressing. The team will ask about the materials bought using the cash assistance and visually check status of the shelter. They will not ask the beneficiary to fill out lengthy templates about their general living conditions or take a photo of the construction. The programme team also decided to have two separate monitoring teams covering different geographical areas. The same teams will be monitoring the same households after three weeks to ensure consistency of the monitoring since photos are not taken, the same staff members are able to verify the progress of the construction.

Unconditional and Unrestricted

Where cash is given to beneficiaries for them to spend on their own specific needs and not for a pre-defined commodity or activity, monitoring might be different. Beneficiary data will still be needed to see how (in general terms, for instance by category) they spent their entitlement and if the programme objectives were met. The intention here is not to monitor the individual beneficiary, but to understand the effectiveness of the program. The overall behaviour of participating beneficiaries is an important indicator to evaluate whether the targeting criteria and amount of cash given were appropriate.

A typical monitoring method is to set up Focus Group Discussions (FGD) with a sample of beneficiaries and non-beneficiaries of the community. With these people an oral discussion is held about the project in general. They are typically asked about their opinion on the project (the targeting criteria, the effects of the project, etc.) Furthermore, they are invited to share their experiences on how the money has been used. From a data protection perspective, oral discussions as such are less problematic than the formal collection of information in paper or digital format. However, it should be carefully considered how the FGDs are recorded. Video and audio records may interfere strongly with the participants privacy. Generally, it is preferable to take meeting minutes. Most likely, this will also make it easier for participants to express their experiences and opinions. When taking meeting notes, there are options to increase the level of privacy. It is worth considering to limit your notes to:

- General discussion points – rather than singling out individuals and their respective comments
- Number of participants and their key characteristics that make them good samples (age, gender, living area) – rather than capturing their full names

The comments may still not be completely anonymous. People taking part in the discussion will know who said what. However, for people consulting the meeting notes later it will be more difficult to

identify a single person behind a certain comment. Of course, it depends on the context whether this limited information would be sufficient for the purposes of the monitoring.

Another monitoring method is to do interviews with a sample of beneficiaries. This is typically done with questionnaire templates. It will be important to check the identity of the beneficiary being interviewed to make sure it is the correct person and that they indeed received the cash assistance. But such identity information may not be necessary to store, so a certain level of anonymity can be maintained. The interviewer will know the beneficiary's identity, but data produced after completing the questionnaire will have more protection from others consulting the data.

Example:

The programme team requests a sample of beneficiaries to participate in a PDM to determine how cash assistance was used.¹⁴ The team checks the ID's of the participants but does not note down their names and ID's in the survey form. In the survey, beneficiaries were open about their dissatisfaction in terms of the encashment because it required them to travel far to reach a money agent, there were liquidity issues with the money agent, and the beneficiaries indicated it would have been helpful to receive in-kind assistance as opposed to cash. Because of the respect for their privacy, their honesty allowed the programme team to learn and adjust for the next cash disbursement, instead of superficially saying they were satisfied in fear of not receiving cash anymore.

Where it is not feasible to keep the identity of the beneficiary anonymous in the questionnaires, it is important to narrow down the questions to the necessary minimum. Templates tend to include a broad range of questions covering various scenarios ("one size fits all"). As explained in Registration chapter, those standardized templates should be tailored to the specific circumstances as needed. Unnecessary questions should be scratched out or deleted.

Try to find options to avoid the use of personal data. If personal data is used for the purposes of monitoring, it is important to identify the legitimate basis for the monitoring and to inform the beneficiary about the handling of their data in the context of monitoring.

Project Decision 2: What beneficiary data can the FSP give me to monitor my programme?

 Data Minimization, Necessity and Data Confidentiality

Project Decision reformulated: What data can the FSP give me for monitoring purposes without invading the beneficiaries' privacy?

Where cash programmes use FSP's, such providers could have data on beneficiaries that might be useful in the monitoring process. Depending on the FSP, some data they may have could include: when money was withdrawn and from where (e.g., ATM or money agents), was money used to purchase from certain establishments (e.g., grocery store vs. liquor store), and signature in the proof of receipt. Getting such data may help speed up and get accurate information on the monitoring process,

¹⁴ Please note that the beneficiaries must voluntarily provide information, they cannot be forced. It should be made clear that their participation will not affect current or future distributions and that they are free to decline participating.

however, from a data protection point of view, this approach could pose certain risks. Payment and purchasing related data could be quite sensitive. Collecting such data from an indirect source (the FSP) rather than the beneficiaries themselves could be viewed as interfering with their privacy.

Personal accounts of beneficiaries

Where the distribution is done via personal accounts (bank/mobile) of the beneficiaries, the National Society by default has no access to these accounts. The FSP, however, can track account movements and maybe willing to share the relevant payment data with you. The question, therefore, is this relevant and what is necessary for the purpose of monitoring? You may want to understand when and how money was used. However, the focus of the monitoring is not on the individual beneficiary but rather on the overall behaviour of all beneficiaries. Hence, it will normally be sufficient for you to receive aggregated payment information. For example, the FSP could let you know:

- the percentage of beneficiaries who spent their money in the first week
- the percentage of beneficiaries who used the money in specific establishment such as supermarket or pharmacies
- the average duration for beneficiaries to fully use the money
- the regions where money has been spent faster
- relative location of money agents and which ones were disbursing more than others

Depending on the context of your programme, you can agree with the FSP what information it should provide you with, keeping in mind the principle of data minimization and necessity.

Example:

A cash programme distributes cash using prepaid cards where beneficiaries can use them to purchase in stores and establishments that accept MasterCard or withdraw from an ATM. The National Society would like to understand what categories of commodities the cash was used for and they check with the FSP if this information could be provided to them. The programme team requests specifically for aggregated data and visualization if (1) cash is being used more to withdraw from ATM's vs. purchasing in stores, (2) the percentage of beneficiaries that have not used their cash assistance yet, and (3) the categories of establishments where the cards were used (e.g., food, medicine, service). The FSP only shares the aggregated data and relevant visualizations rather than specific data on purchases and which person transacted where and when.

In practice, and if not previously negotiated, the FSP might not be willing to create the specific reports or give too specific information for you since this is an additional effort. If this is the case, another option is to ask the FSP **not** to send you the full set of payment data and only very limited transactional information to protect the beneficiaries' privacy. The FSP should be asked to eliminate names and card numbers for each financial activity.

If the only option is to receive the full raw transactional data from the FSP, it is advisable to limit who receives and accesses the full data and have this person be the "gatekeeper" within your team. The FSP shall send the payment data only to this one person. The gatekeeper can then extract only the

necessary information for the rest of the programme team to process. The gatekeeper can then securely delete the full data received by the FSP, so it is not inadvertently used for something else. Abstract aggregate information offers higher level of data protection and in many cases could be sufficient.

Example:

A cash programme distributes cash using the mobile money wallets of the beneficiaries. The National Society would like to understand which mobile money agents were used for encashment so they can notify the vendors before the next distribution in case there are liquidity issues. The FSP is not able to give just this information but willing to send the full transaction list with all the financial activities of each individual beneficiaries and where they are encashing. The programme team informs the FSP to send it only to the IM manager supporting the cash programme who will then extract the necessary data for the programme team to process. The IM manager deletes the file after extracting only the data aggregated data needed by the team.

Virtual account of National Society

Where the distribution is done via virtual accounts of the National Society (see FSP chapter), the FSP may not have direct link between the transactional data and the actual beneficiaries, since the management of the sub-accounts is done by the National Society. Consequently, having direct access to the transactions of the beneficiaries because you are the account owner, might pose some risks to privacy. As discussed, individual payment data is sensitive and for the purposes of monitoring it is normally not necessary to know about individual beneficiaries but rather the group of beneficiaries as a whole.

One option to protect the beneficiaries' privacy again is to designate a "gatekeeper" who alone will have access to the full transactions available in the platform. If only one person of the team accesses the platform and transforms the individual information into abstract information, the data protection risk could be reduced. Where a gatekeeper is not possible to designate, it is the responsibility of all team members that have access to the platform and full set of data, to respect the confidentiality and privacy of the beneficiaries and make sure that sub-account identifiers are not linked back to individuals – this makes it crucial that all team members have good familiarity with data protection practices and principles.

Try to monitor the programme without receiving personal beneficiary data from the FSP. Whenever you receive such data, it is important to inform the beneficiary about this and to explain how you intend to protect the beneficiaries' privacy.

Project Decision 3: What beneficiary data can the merchant give me in a voucher programme?

 Data Minimization, Necessity and Data Security

Project Decision reformulated: What data can the merchant give me for monitoring purposes without invading the beneficiaries' privacy?

In voucher-based programmes, transaction data from merchants might be used in the monitoring. The merchant will have records on how many vouchers were redeemed in which timeframe, and they will also have records of commodities selected in exchange for the vouchers. However, it is still important to ensure a high level of data protection when utilizing such information. It is generally sufficient to review aggregated data of the general use of vouchers and the commodities purchased. For the purposes of monitoring, it is not relevant what a single beneficiary used the voucher for. What is important is to understand the overall behaviour of the participating beneficiaries to evaluate the effectiveness of the programme. It should, hence, be avoided to review data that allow to identify when and where an individual beneficiary bought a certain product. This can be done by asking the merchant to aggregate the data for you. If it is not possible, request only for limited data set with no identifiers. Otherwise, like the previous sections, try to designate a “gatekeeper” within your team who will receive and extract only the relevant set of data, and immediately delete the full transactions list.

VIII. General Guidance

This section looks at key data protection considerations that are applicable throughout the cash programme.

Data Protection Considerations

Data Storage

When collecting personal data of the beneficiaries it is extremely important to keep them safe and protect them.. This means to take sufficient security measures to avoid a so-called data breach (loss, unauthorized access, etc.) (see below for guidance on what to do in case of a data breach).

IT-solutions for data security are very technical and often require expert knowledge. Therefore, it is recommended to develop a coherent cross-programme approach together with your IT Management if possible. The concept can address data flows, the channels and interfaces for exchanging data, encryption levels when data is stored and transferred, backup or redundant storage to prevent data loss, and the access controls to ensure only authorized individuals are using the data, etc.

In any event, the following aspects should be considered carefully:

- For digital data, wherever possible it is key to use robust database or data management solution. Storing data in publicly available repositories such as Google or Dropbox should be avoided at all times. The use of databases has many advantages, because they offer technical security, such as native encryption, password-protected containers/folders, log-file tracing, backups, etc. Data management solutions (such as RedRose and LMMS) can integrate with different data collection tools such as ODK/Kobo and payment mechanism such as mobile money or banks for cash transfer. It is important to evaluate such solutions in terms of data security to ensure data is protected whether it is in transit (e.g., when using mobile data collection such as ODK/Kobo and data is uploaded from the mobile phone to the data management server) or at rest (when data is stored in the cloud server).

The physical storage location of data should also be evaluated against the national laws (i.e., some countries prohibit, or place limitations on, the transfer of personal data outside of their jurisdiction).

- Where data must be stored on laptops or USB-sticks, the risk of loss and theft is higher than in a proper database. Additional security measures should be adopted to limit this risk. The hardware should ideally be protected by hard-drive encryption (e.g., Bitlocker by Microsoft). Furthermore, you can add an additional level of protection by encrypting or password-protecting the documents on the hard drive. Laptops and USB-sticks should also be physically secured by using laptop locks and keeping them in a locked drawer when not in use.
- When creating a password try to use strong passwords that are not easy to guess. Good practice is to use small and big letters, digits and special characters and to change the password regularly. Avoid sharing accounts and passwords. If the account is generic (e.g., generic email boxes administered by multiple people), it is important to limit the number of people (see below – Access Control).
- Paper files have an even higher risk of loss and unauthorized access. If paper files are the sole option, store them away in a repository with a lock. While using them, it helps to limit the visibility by third parties.

For more tips, please see the [IFRC's IM Data Protection Flyer](#) providing do's and don'ts on storage and processing and the [IFRC's information security policy](#).

Data Retention and Deletion

What happens to the beneficiary personal data after the programme is completed? Ideally, they are not left in paper files or in a database for an unlimited period. Once data from a specific programme is no longer needed, it should be deleted, or at the very least aggregated or anonymized. If needed for an extended period but does not require regular access (such as audits), then archiving in an offline and secure manner could be an option.

Retention Periods

It is recommended to have a time-limited retention period in advance, defining how long data should normally be stored. Once the retention period expires, the data is deleted. Only if there are compelling reasons that require further retention, the data can be kept for a longer but limited time period. Retention periods can be embedded in databases to allow automated purging of data. If you want to learn more about those options, please consult with your IT colleagues in your organization. If databases or automated retention periods cannot be used, another option is to set calendar reminders. The aim is to actively think in regular intervals about whether to keep or to destroy data that is no longer needed. The length of retention periods depends on the programme itself but could also be dictated by your own organization's policies. When designing the CVA intervention, the appropriate retention periods should be considered so they can be communicated to the beneficiaries. Some aspects to consider are:

- the length of the project
- the sensitivity of the data
- the scale of the planned monitoring
- the likelihood of follow-up issues

Other purposes

Even if the programme has been closed and the monitoring has been done, it might seem useful to keep certain data for other purposes. Firstly, they could be used to create additional **reports and statistics**. However, for this purpose it is generally not necessary to keep data that identifies individuals directly (e.g., names, ID numbers). It is sufficient to generate a condensed set of aggregated data. Secondly, particularly for areas prone to the same hazards, it is likely that the data might be useful in **general preparedness for future, similar programmes** (e.g., recurring hurricanes or typhoons). In those situations, it might seem reasonable to simply keep the data. However, data tend to have a limited lifespan. For new programmes they need to be updated and verified. People leave or move to the area, their living conditions change, children are born, or family members die. Hence, the retention of data for a potential new programme is very often not useful. If you decide to keep the data for a future programme, it is also important to think about whether the new purpose is compatible with the original purpose. Humanitarian purposes may be compatible, but if the purpose is not compatible, it is key to inform beneficiaries about your intention to reuse the data for another purpose and to identify a new legal basis for this new processing (see Legitimate basis section of the Registration chapter). Thirdly, data might have to be stored for **audit purposes**. If so, audit requirements normally name required storage periods. If not, a reasonable storage period can often be identified by looking at the timeframe and/or purpose of the audit. Data stored for audit purposes should be archived separately from other data flow.

Non-Beneficiary Data

In the process of targeting, you collect personal data from people who in the end may not benefit from the assistance because they do not meet the eligibility check (see Targeting chapter). Similarly, during beneficiary registration, you might have collected data from people that eventually show to be ineligible. The storage of personal data of those non-beneficiaries must be considered very carefully. Since they will not participate in the programme, their data is no longer needed once the eligibility check is completed. Nevertheless, it might be in your interest and even in the interest of the non-beneficiaries to keep their personal information for a certain period of time. One reason could be to have evidence of the decisions if the non-beneficiary launches a complaint against the National Society for having been excluded in the programme. In this situation, it can be very helpful to be able to see how this was decided and what data points were used in the decision. If possible, in situations like this, store the respective information separately from the rest of the other eligible beneficiaries. The idea is that this data is no longer part of the data flow in the ongoing programme. But, if a complaint comes up, it can be retrieved.

Access Control

The information collected directly from the beneficiaries or from other sources (governments, etc.) should be treated confidentially. Confidentiality is closely related with the principles of data minimization and necessity and data security as explained above.

Cash programmes typically involve different stakeholders: internal (e.g., direct programme and field teams, support services such as colleagues from Finance, Logistics, IM, and IT, and managers) and external (e.g., FSP, donors, government, other NGOs). We have already looked at handling personal data with external stakeholders (see chapters on FSP and data sharing with externals). For internal stakeholders, it is important to determine the type of access and the level of access required with regards to beneficiary data. Some organizations have an information classification. For instance, the [IFRC's information security policy](#) categorizes beneficiary data as confidential or highly confidential

depending on the context; this requires the highest level of security protection as well as limited access on “need to know basis”.

Some ways to ensure proper access control:

- Use username and password to access the database or data management platform. Inform users not to share their username and password to others. Also, avoid creating generic users where multiple people can login as that user. Actions of every user should be auditable and traceable.
- Utilize role-based access control (RBAC) which means users are given specific roles and each role gives access to certain functions and data in the system. The access could be as granular as necessary (e.g., access to the beneficiary list, ability to download beneficiary list, or just giving access to aggregate data such as dashboards). Access should be revoked if there is a security issue with a user.
- Have an access log to record everyone who is logging in and accessing certain pages or data, as well as a download log for those downloading data directly from the system (noting that this is also considered collection and processing of personal data and must be treated appropriately).
- When downloading data in an Excel spreadsheet, add password protection or encrypt the file.
- If there is no database, files should be password protected and only authorized personnel should have access to the files. For paper files, only authorized staff should also have direct access and files should be kept in a locked container.

Examples:

The cash programme involves 10 staff members and volunteers for implementation. While 3 are responsible for targeting and beneficiary registration (Team 1), the other 7 are only responsible for contacting service providers and the distribution of cash (Team 2). Team 2 does not need to know about the vulnerability of beneficiaries. They only need to know about such personal data, that are necessary for the cash part of the project (names, bank accounts, KYC). Therefore, a list of beneficiaries with limited information is generated for them by Team 1. All other information is stored in a password protected database and only Team 1 has this password. Furthermore, only 1 person has the role of the admin and can fully access to the database (read and write access), while the other two team members have read-only access.

In the same scenario, the distribution method is cash in envelopes. It is expected that Team 2 will have to justify the choice of beneficiaries on distribution day. If such a situation comes up, it is necessary for Team 2 to have access to the supplementary information. Therefore, they request the additional information from Team 1 who generates the additional limited information.

Transmission process (Data sharing)

When sharing data, the transmission process may increase the risk of data loss and unauthorized access. Therefore, when transferring personal data, security measures play an important role.

- Ideally data is shared using **secured tools** such as secure FTP with username and password and limited access to download data from the secure database or data management platform.
- Where communication regarding beneficiaries may need to be sent via **email**, it is important to remember to: (1) limit the number of recipients, (2) password-protect the attachments and (3) encrypt the emails (when possible). This offers some protection in case emails are hacked or email sent accidentally sent to a wrong address. The risk of exposing beneficiary data to unauthorized persons is reduced when emails and attachments are encrypted. If unsure how to encrypt files or emails, please contact your IT colleagues. Sending emails to mailing lists rather than to individuals may seem convenient but could be problematic if you do not know exactly who is included in the mailing lists. Same is true when sending to generic email addresses where there could be different people with the password or managing the generic email account. Take caution also when emails are forwarded or when email chains are created by having people reply to the messages. As the recipients grow or change, ensure that the new recipients are also authorized to be informed of the beneficiary personal data.

For example:

The situation of certain potential beneficiaries is discussed via email with the community leaders to decide whether they qualify for the cash program. The email can be sent to the community leader who helps in the decision making and to colleagues involved in the targeting. However, it should be avoided to send the email to a generic email address such as "info@community" or "cashteam@".

- Be careful if you want to share files containing personal data via **mobile messaging applications**, such as WhatsApp. Unless you are confident in the security of the messaging app (for example, Signal is widely considered to be significantly more secure than WhatsApp), **do not use it** to share personal or other sensitive data (whether of staff, volunteers or beneficiaries).

Handling of Data Breaches

Despite all security measures there is no guarantee that a data breach can be prevented in all situations. As defined in the beginning of this guidance, a data breach *means the unauthorized access to, or destruction, loss, alteration or disclosure of personal data*. Once a data breach has occurred, it is important to take the right steps to remedy the consequences of the breach. It is recommended to make yourself and your staff aware of these steps in advance of a breach. As soon as you become aware of a breach, make sure to:

- **Report without undue delay** to your manager or supervisor as well as the Data Protection focal point, the legal team or another person in charge of data protection in your National Society. If you do not know who is responsible, communicate your concerns to the leadership in your organisation.

The following steps should then be performed in cooperation with these experts:

- **Investigate the extent of breach:** What kind of breach? What kind data? How much data? Duration of breach? Which data subjects? Exposure of data to whom?

- **(in parallel) Take mitigating measures** (depending on the kind of breach, *e.g.*, cut IT-systems, retrieve back-up data, contact unauthorized person to end exposure of data, close loopholes, inform partners involved and potentially donors.
- **Evaluate level of risk for data subjects and make reasonable efforts to inform data subjects if risks are high** for transparency reasons.
- Depending on national laws, **consider informing data protection authorities in your country.**
- **Prepare report/lessons learned** and **eliminate identified organisational or technical weaknesses.**
- **Improve response plan for next incidence** as necessary based on experience gained.

Briefing of Staff and Volunteers

The first step towards effective data protection is awareness. Therefore, it is important to make your staff and volunteers aware of the key principles of data protection and how to address them in the CVA programme cycle. It is recommended to hold regular training sessions on data protection particularly for those new to the organisation as part of their onboarding. Training materials could be prepared in advance for onboarding and as a refresher for those who have been trained before. In this training, the importance of data protection should be highlighted and the key principles explained. And more importantly, what data protection considerations should be addressed within the CVA processes and responsibilities of staff and volunteers depending on their roles. There should also be awareness on how to respond to data breaches.

Analysing and Monitoring Data Protection Risks

To make data protection a true safeguard for the beneficiaries' privacy in your programmes, it is strongly recommended that you note down the data protection considerations you perform. Why? Because it helps to set up a structured and consistent approach to manage risks and find a good balance. Also, documenting risks and decisions taken will be important in case an audit or investigation is necessary.

There are some tools that could be used in analysing and documenting risks related to data protection:

Risk Matrix and Risk Register. The CiE toolkit covers risk analysis in Preparedness (Module M1_1 Prepare and Analyse), Assessment (Module M2_4), and Response Analysis (Module M3_1_4). Additional risks described for Cash for Work and Voucher programming also. The same risk matrix and risk register could be used to ensure data protection elements are reviewed along with the other types of risks. A new category for data protection may need to be created to categorize the risks appropriately. Analysing such risks and creating mitigation measures will be important. And as the programme runs, the risks should be reviewed and updated as necessary.

Data Protection Impact Assessment (DPIA).¹⁵ This is a formal tool to document data protection considerations for risks identified as well as foreseen mitigation measures. Its preparation might require external consultation and the inclusion of relevant stakeholders such as your legal colleagues. The performance of such an in depth DPIA is not necessary in all cases particularly when running similar CVA programmes. It might be necessary when new methods, technology are used where impacts to beneficiaries are not yet known. It would also be helpful when there are potential concerns from community members in terms of handling their data, to determine where the actual risks are and if they could be mitigated.

¹⁵ See for more details in the [Handbook on data protection in humanitarian action](#). Also, a DPIA template can be found in the reference section of this guidance.

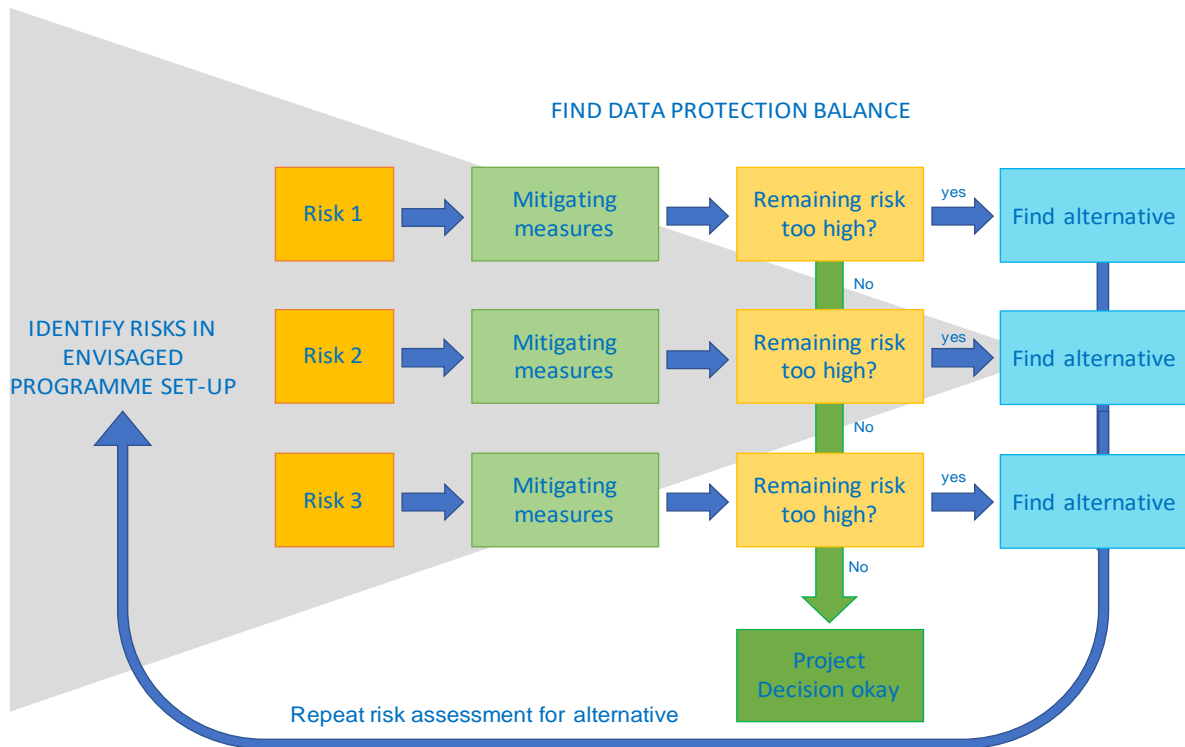


Figure 4: Balancing risks and actions related to data protection

Figure 4 aims to help the thinking process on evaluating data protection risks. This involves identifying and noting down the risks and possible mitigating measures, determining the level of the risks (based on impact and probability) and finding alternatives to take into account. For example:

Inclusion of FSP?

- > Risk 1: Use of data for other purposes besides what have been agreed on
- > Mitigating measure: prohibit in contract
- > Remaining risk too high? Yes, because FSP’s reputation and reliability are questionable
- > Alternative: other FSP, cash in envelopes or in-kind
- > repeat risk assessment for alternative

If an initial assessment of the risks reveals that the programme setup presents high data protection risks, it is advisable to perform the assessment using a formal DPIA format. The obligation to perform a formal DPIA is with the organisation leading the programme, in the case of implementation partnership.

The performance of a formal DPIA should be considered (and under some data protection laws may be required), for example, in the situations listed below. Please note: All these ways of data processing are strictly subject to the principle of data minimization and necessity. A DPIA cannot justify unnecessary processing of data.

- New technology is being used to collect, administer, or store personal data (cloud storage, geolocation, social media, etc.). Not knowing how modern technologies work

could increase the risk of unauthorized access (hacking) and open possibilities to unauthorized surveillance.

- Individuals may be subject to automated decision making or profiling. Automated decision making interferes strongly with data protection, because decisions are being made beyond the control of the individual and without a possibility for the individual to retrace and discuss the decision. Profiling is problematic because creating a profile of persons is like putting them in certain categories without real prior interaction with the individual.
- Personal data might be transferred to a third party (or country) without similar data protection standards. As discussed, sharing data might result in losing control to how that data is used. It should only be done where the other party has an adequate data protection standard. If this is not the case and data must be shared anyway, it is important to thoroughly evaluate whether this would be too much of a risk for the beneficiaries (category of data, protection standard, etc.)
- Sensitive data, such as data about health status or religious orientation or biometrics might be processed on a large scale (number of persons, variety of data, duration of processing, geographical extent, etc.). This data is highly sensitive since they relate to very personal and private aspects of someone's life. In addition, this kind of information in the wrong hands can be very detrimental for beneficiaries.
- Mass surveillance might be part of the programme. Mass surveillance interferes strongly with the rights of all persons concerned, since it is an important part of privacy not to be subjected to constant control of others or automated systems.
- Consolidation and cross-linking of data from different sources might occur. The combination of various datasets on one individual increases the risk for the individual's privacy.

Independent from the format, the risk assessment should be performed prior to the start of the programme, together with the general risk assessment for the programme as described in the CiE toolkit.

If there are questions and concerns regarding data protection, do not hesitate to communicate to your manager and/or your legal team. You may also send your queries to the [Cash Hub](#), which is a Movement-wide resource for CVA. The Cash Hub supports cash practitioners and offers materials including lessons learned from other National Societies and may have considered similar questions from other Movement partners in the past.

Community Engagement and Accountability (CEA)

As discussed in all the chapters, informing beneficiaries and having a help desk and feedback mechanism are important aspects of implementing data protection. Where beneficiary communication is done by a separate CEA team, it is important that they are aware of the data protection considerations and ensure they have information to address questions about data protection or know how to refer those questions to someone who could answer.

IX. References

Policies and Guidance

- [Handbook on data protection in humanitarian action](#) by ICRC and Brussels Privacy Hub
- [IFRC Policy on Data Protection](#)
- [ICRC Rules on Data Protection](#)
- [ICRC Policy on the Processing of Biometric Data](#)
- [IFRC's information security policy](#)
- [IFRC's IM Data Protection Flyer](#)

Templates and auxiliary material

The following materials need to be contextualized by the National Societies to meet requirements unique to them; in particular, adherence with their national data protection laws and policies which might be stricter than the standard of data protection applied when preparing these documents.

- [Financial Service Provider standard contract template](#) (working draft)
- [Financial Service Provider pre-contract questionnaire/due diligence template](#) (working draft)
- [DPIA template](#) (working draft)
- [Sample Privacy Notice template](#) (working draft)