Governance Framework for Data Stewardship

Template and Guidance

Preamble

The humanitarian sector collects an increasingly large amount of data from and about individuals, households and communities affected by crisis. Humanitarian organisations are often required to share some of that data in order to achieve collective goals.

Data sharing for humanitarian operations ought to operate within frameworks that ensure privacy, data protection, interoperability, data analytics, data security, community engagement, capacity building, and ethical use of technology.

This template Governance Framework for Data Stewardship was developed by the Collaborative Cash Delivery Network to support their interoperability pilot projects to improve data governance within the humanitarian sector.

The Framework is intended to facilitate a collective approach to responsible data management, and to move towards inclusion of beneficiary voices into such a collective approach. It draws on recent research and practice in Data Stewardship.

The template should only be utilised in consultation with appropriate country office management, information technology/digital teams, and local and home office legal counsel at each participating organisation.

The template requires discussion and modification for each specific context and party. In addition to the text body, careful attention should be paid to the footnotes, which are intended to assist the reader in analysing the points at issue in the template.

The template, once modified and agreed, is a legally binding instrument for the signatories who participate in the data sharing initiative described in the instrument. This instrument is to be implemented in a progressive manner according to Schedule A.

The instrument should be accompanied by a Multi Party Data Sharing Agreement, a template for which has been developed by CCD as a separate document. Other instruments should be added as necessary to meet the requirements of the signatories.

This instrument outlines the principles, processes, and administrative structures to be established to facilitate effective and accountable data stewardship initiatives. **In line with the above, the Data Governance Framework states as follows** –

Part One: Preliminary

1. Guiding Principles

This Framework has been developed on the basis of, and its implementation should be guided by, the Principles for Data Responsibility in Humanitarian Action in the IASC Operational Guidance on Data Responsibility, and the Basic Principles in the ICRC Handbook on Data Protection in Humanitarian Action (Second Edition).

Organisations implementing a data stewardship initiative are recommended to read these documents in full. A complete description of the Principles for Data Responsibility is given in Annex A to this Framework. In summary, where an organisation processes data, the following principles shall apply:

a. Accountability
b. Confidentiality
c. Coordination and Collaboration
d. Data Security
e. Defined Purpose, Necessity and Proportionality
f. Fairness and Legitimacy
g. Human Rights-Based Approach
h. People-Centered and Inclusive
i. Personal Data Protection
j. Quality
k. Retention and Destruction
l. Transparency

2. Applicable Law

a. The organisations implementing this Framework shall be guided by the laws of the Country, including any relevant constitutional law, case law, or regulations including, but not limited to, data protection, data privacy, cyber security, digital rights, and so on.

b. The organisations participating in this Framework shall ensure that they comply with the laws and regulations described above, and also with any other laws, policies, and regulations that they are legally obligated to comply with, including if relevant those of the countries in which their global offices are incorporated.

3. Definitions

"**Affected Population**" means people affected by emergencies, crises, conflicts, and natural disasters around the world.

"Consent" means any freely given, specific and informed indication of an agreement by the data subject to the processing of their personal data.

"**the Country**" means the country within which, and under whose jurisdiction, the Data Steward is operating.

"**Data**" means information represented in a formalised manner which is processed in relation to humanitarian operations.

"**Data Host**" means the Data Host established under Article 8 of this Framework.

"Data processing" means any operation or set of operations performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"**Data Steward**" means the Data Steward established under Article 7 of this Framework.

"**Data Sharing Agreement**" (hereafter "**DSA**") means the agreement governing data sharing between the Members and the Data Host.

"**Data stewardship initiative**" includes any policy, plan, goal, action, or **omission** relating to data use under this Framework.

"**Data subject**" means a natural person that is the subject of personal data processing, for purposes of this Framework, a member of an affected population.

"Focal point" means an individual assigned by their organisation to represent the interests of that organisation to the Data Steward, and to represent the work of the Data Steward to their organisation.

"**Framework**" means this Data Stewardship Governance Framework.

"**Member**" means an organisation operating in the Country which is also a member of the Data Steward, as described in Article 6 of this Framework.

"**Organisation**" means a humanitarian organisation operating in the Country to provide services to affected populations.

"**Oversight Committee**" means the committee established under Article 9 of this Framework.

"**Representative**" means an individual selected to represent the collective interests of the Data Steward on the Oversight Committee.

4. Purpose Limitation

Bearing in mind the above principles, the data referred to in this Framework is that data which Members shall individually and collectively process only for the purposes of:[1]

a. deduplication of data,
b. referral within or between organisations, and
c. any other functions agreed upon by the Data Steward.

A full description of these purposes, including the amount and extent of data which shall be processed, and the period for which that data shall be retained, in order to achieve these purposes, should be included in Schedule C.

5. Localisation[2]

Data for purposes of data stewardship initiatives under this Framework shall be processed and stored within the Country.

Part Two: Data Stewardship

6. Member Organisation

a. A Member shall be either –

i. a humanitarian organisation working in the Country,

[1] The Members should list all relevant purposes in brief here, and describe them in full in Schedule C.
[2] This clause is meant to improve accountability by ensuring that data subjects' data remains in the jurisdiction (i.e. the Country) within which they have legal recourse as individuals. Since most platforms, and the data stored on them, are now hosted in the cloud rather than on local servers, this may not be possible, and the Data Steward should make a decision based both on the local situation and the capabilities of the Data Host.

ii. an organisation representing affected populations in the Country which are are served by any Member, and through data collection by that Member are considered to be data subjects,[3]
iii. any other organisation considered necessary and appropriate by the existing Members to ensure the Data Steward can achieve its purposes.

b. A Member shall –

i. sign the DSA agreed upon by the Members which shall govern the practice of data sharing within the Data Steward,
i. commit to compliance with this Framework by signing and implementing it, and ensuring their organisation supports it,
ii. participate in data stewardship initiatives for the specific purposes described in this Framework,
iii. assign a Focal Point to represent the Member within the Data Steward,
iv. assign a Representative to the Oversight Committee if necessary,
v. provide support, technical, and strategic guidance to the Data Steward, the Data Host, and the Oversight Committee,
vi. ensure that their data management policies and practices are in compliance with the this Framework and the DSA,
i. ensure that their staff have sufficient capacity to participate and support in data stewardship initiatives,
vii. provide data subjects with adequate information regarding data stewardship initiatives, to include:

- which data is to be included in data stewardship initiatives, for what purpose that data will be used, and for how long it will be held.
- which organisations are involved in data stewardship initiatives, and any changes in such organisations.
- the purpose of data stewardship initiatives, and their intended effect on humanitarian service provision.
- their rights as data subjects, and through which mechanisms they can assert those rights.

c. An organisation may exit from data stewardship initiatives by giving notice to the Data Steward. Once ratified by the Data Steward, the notice shall take effect one month from the date of the resolution by the Data Steward.

[3] The intention here is to ensure that the interests of the data subjects are represented in decision making by the Data Steward. Here that representation is achieved by an organisation representing their interests by proxy, but it could also be achieved through some form of direct representation where appropriate.

d. The Data Steward may suspend or remove an organisation from data stewardship initiatives[4] if that organisation –

   i. ceases operations in the Country,
   ii. without reasonable cause declines to engage in data stewardship initiatives for a period of three months or more,
   iii. violates provisions of this Framework and declines to address the violations within a period of three months or more, or
   iv. collects, processes, stores, shares, and transfers data shared within data stewardship initiatives for reasons not within this Framework.

7. Data Steward

a. The Data Steward shall be the entity which consists of the Members, acting through the structures defined in this document.

b. A Member shall be any organisation which meets the requirements of Clause 6a, which has signed this Framework, and whose membership has been approved by the Data Steward.

c. There shall be at least one Member of the Data Steward representing data subjects specifically or affected populations more generally.[5]

d. The Data Steward shall act in the interests of the data subjects, protecting and promoting their individual and collective data rights, while at the same time safeguarding the legitimate interests of the Members of the Data Steward.

e. An organisation may become a Member of the Data Steward through two means:

   i. by nomination by an existing Member,
   ii. by application through a written statement.

[4] The Data Steward will need to reach agreement with the suspended or removed Member concerning how long the data contributed by that Member will remain on the platform for the purposes of the data sharing initiative.

[5] More than one data subject representative may be included in the Data Steward, depending on the size and needs of the Steward. Such representatives may be, inter alia, individuals directly representing a community or region (such as a community leader or mayor), individuals with particular authority to speak on behalf of data subjects (such as a rapporteur), organisations working closely with those communities (such as religious institutions), or simply local civil society or community-based organisations. These representatives should be asked to join, and asked to act, in the spirit of ensuring proper representation of the interests of data subjects.

f. A Member that is signatory to this Framework shall be represented to the Data Steward by an officially designated Focal Point, authorised to make decisions on behalf of that organisation.

g. Members shall ensure that their Focal Point is always designated, and shall immediately replace any Focal Point unable to perform their function for any reason with a new Focal Point.

h. The Data Steward shall have powers to deliberate and vote on –

   i. ratification, amendment, suspension, or termination of this Framework,
   ii. inclusion into the membership of the Data Steward,
   iii. suspension or removal of a Member from the Data Steward,
   iv. designation and dismissal of a Data Host,
   v. appointment of Representatives on the Oversight Committee,
   vi. reports from the Data Host and the Oversight Committee,
   vii. reports from Members representing data subjects or otherwise affected populations, and
   viii. election of a Chair, a Vice-Chair, and a Secretary of the Data Steward who shall not be the Data Host or a Representative on the Oversight Committee.

i. The Data Steward shall take decisions based on voting by Members:[6]

   i. A Member shall have one vote at the Data Steward.
   ii. Decisions will be made by a simple majority vote.
   iii. Voting shall be by acclamation or secret ballot, depending on the sensitivity of the vote.
   iv. A decision for ratification, amendment, suspension, or termination of this Framework shall be ratified by at least half the Members of the Data Steward through secret ballot.
   v. A decision on designation of a Data Host shall be ratified by at least half the Members of the Data Steward.
   vi. A decision to suspend or remove a Member shall be ratified by at least half the Members of the Data Steward.

j. The Data Steward shall hold meetings:[7]

[6] The Members may decide that Points iv-vi should have a higher voting threshold, given the sensitivity of the issues involved and the implications of a change in Data Host or the removal of a Member.
[7] The Members may decide that the frequency of meetings needs to be adjusted depending on circumstances, e.g. during a period of high activity the Steward may need to meet more often.

i. at least once every month until an Oversight Committee is established.
ii. at least once every six months once an Oversight Committee is established.
iii. on an *ad hoc* basis in case of an emergency, or at the request of either a Member, the Oversight Committee, or the Data Host.

k. The Agenda for a Data Steward meeting shall be sent to Members at least ten (10) working days before the date of the meeting and a Member shall send any motion to the Chair at least five (5) working days before the date of the meeting.

l. The quorum at a Data Steward meeting shall be at least half the total number of Members.

m. The agenda of a Data Steward meeting shall include, but not be limited to,

i. adoption of the agenda of the present meeting and the minutes of the previous meeting.
ii. the Chair's report, including reports from the Oversight Committee and Data Host.
iii. reports from the Member(s) representing data subjects or affected populations.

n. The Data Host shall provide the Secretariat role for the Data Steward, with the Secretariat functions agreed upon by the Members.[8]

8. Data Host

a. The Data Steward shall designate a Data Host from within its membership.

b. An organisation may become Data Host through two means:

i. by nomination by an existing Member,
ii. by application through a written statement.

c. Any Member that is being considered for the role of Data Host shall submit to the Data Steward:

[8] The Secretariat role can be played by any Member. The Data Host is mentioned here as a default option since any organisation acting as Host is likely to have sufficient resources to provide Secretariat functions in addition.

i. written notice of their intent to act as Data Host, and
ii. evidence of their institutional and technical capability to uphold the principles described in this Framework, including those of privacy and data security.

d. A Member will assume the role of Data Host following a simple majority vote by the Members.

e. The Data Host shall act on behalf of the Members, allocating staff and other resources as necessary to fulfil the following tasks:

i. to host and maintain the technical platform,
ii. to host and safeguard the aggregate data,
iii. to manage access to both of the above.

f. The aggregated data hosted by the Data Host will be considered to be the collective responsibility of the Members.

g. The Data Host shall submit quarterly reports[9] to the Oversight Committee that shall include:

i. analytics of platform use, including usage statistics by Members and Data Subjects,
ii. a summary of the catalogue of data contained in the registry maintained by the Data Host,
iii. a summary of all data stewardship activities undertaken by the Steward,
iv. a summary of all data breach and other security incidents experienced.

h. A Member shall act as a Data Host for a minimum term of one year,[10] renewable without limit at the discretion of the Data Steward.

i. A Member shall cease to act as Data Host where:

i. their term under this Framework lapses and they do not wish to continue to act as Data Host,
ii. they cease operations in the Country,
iii. they decline to carry out their mandate for a period of two weeks or more without reasonable cause,

[9] The Data Steward may decide that the frequency of reporting needs to be adjusted depending on circumstances, e.g. if there has recently been a security incident which the Data Host is addressing.
[10] This minimum term may be amended by the Data Steward depending on the specific needs of the Members.

iv. they violate provisions of this Framework and decline to address the violations within a period of one month or more, or
v. they collect, process, store, share, and transfer data shared within the Data Steward network for reasons not within the ambit of this Framework.

j. i (iii – v) shall require a resolution of the Data Steward.

k. Where a Data Host ceases to act the Data Steward shall designate a Data Host on an interim basis, or on a term basis as per this Framework,

l. The Member that ceases to act as Data Host shall provide

i. to any successor Data Host designated by the Data Steward, access to all platforms and data held under this Framework, and
ii. to the Oversight Committee, a comprehensive report of all its activities under this Framework.

9. Oversight Committee

a. An Oversight Committee designated by the Data Steward shall oversee the operations of the Data Host on behalf of the Members.

b. A Member may volunteer to act as a Representative on the Oversight Committee, or may be proposed as a Representative by any other Member.

c. No more than two Representatives on the Oversight Committee shall be from the same Member.

d. The Data Host may not be a Representative on the Oversight Committee.

e. The functions of the Oversight Committee include –

i. monitoring Members' compliance with the provisions of this framework, particularly regarding the rights of data subjects,
ii. monitoring the progress of data stewardship initiatives, including establishing metrics for success with regards to specific purposes,
iii. providing strategic direction and oversight regarding the performance and compliance of the Data Host,

iii. establishing feedback mechanisms through which data subjects may submit requests or complaints
iv. strengthening otherwise the agency of data subjects over their data, and
v. appointing auditors to audit data stewardship initiatives under this framework.

f. The Oversight Committee shall submit quarterly reports[11] to the Data Steward that shall include –

i. a summary of the performance of the Oversight Committee and the Data Host, including any issues arising,
ii. a summary of feedback received by the Data Host or the Oversight Committee, including matters resolved and outstanding,
iii. a list of organisations who have access to data in the Data Host's custody, and which data they have access to,
iv. risks and challenges experienced and strategies employed to mitigate them.

g. The Oversight Committee shall be composed of five Representatives[12] –

i. four Representatives representing humanitarian organisations, and
ii. one Representative representing data subjects or the affected population.

h. A Representative on the Oversight Committee shall –

i. have practical knowledge and experience in the humanitarian sector, or
ii. technical knowledge on data governance, or
iii. experience working with the affected population.

i. A Representative on the Oversight Committee shall serve for a term of one year, renewable once.

j. A Representative on the Oversight Committee shall be removed and replaced if –

[11] The Data Steward may decide that the frequency of reporting needs to be adjusted depending on circumstances, e.g. if there has recently been a security incident which the Oversight Committee is addressing.
[12] The Data Steward may choose to expand the Oversight Committee on a temporary basis - for example to add specific expertise required for a set period - or on a permanent basis - for example if the Data Steward membership and operations have grown significantly and require wider representation. The composition of the Oversight Committee may also be altered at the agreement of the Data Steward, for example to increase the representation of data subjects.

i. they are unable to act as Representative through illness, death or any other persistent absence,
ii. they resign their position within the Member, or the Member which they represent decides to replace them as their Representative, or
iii. they violate the provisions of this Framework without reasonable cause.

k. The Oversight Committee may constitute *ad hoc* subcommittees to deal with matters arising out of compliance and implementation of this Framework.

Part Three: Data Subjects

10. Data Subject Rights

a. A data subject shall enjoy data subject rights including:

i. the general rights and freedoms and specific data subject rights set out in the constitutional and legislative framework of the Country,

ii. the right to be informed of the purpose for which their data is being collected, processed, stored, shared, and transferred,

iii. the right to object to or restrict the collection, processing, storage, or transfer of their data,

iv. the right to be provided with copies of data about them that is held by Members or the Data Host individually or collectively,

v. the right to data portability,

vi. the right to have their data corrected and erased where necessary,

vii. the right to file complaints regarding their data,

viii. the right to be represented by a person of their choice, and

ix. the right not to be subjected to automated decision making.

11. Accountability Mechanisms

a. The above rights shall be exercised by making requests, demands, or complaints to a Member, the Data Host, or the Oversight Committee, depending on the nature of the complaint.

b. A data subject aggrieved by any action, omission, or decision made under data steward initiatives, shall in the first instance and where applicable be encouraged to file a complaint with the respective Member.

c. Where a complaint does not concern a specific Member, but relates to data stewardship initiatives, the aggrieved person shall lodge a complaint with the Oversight Committee.

d. The Oversight Committee, working with the Members as necessary, and taking into account the infrastructure and capability constraints on the data subjects, shall establish:

i. appropriate channels or fora for informing data subjects of their rights under this Framework;
ii. appropriate channels or fora for receiving any form of requests or feedback from data subjects,
iii. appropriate mechanisms for addressing any requests or feedback received from data subjects, and
iv. appropriate measures for responding to or resolving such requests or feedback, both directly or indirectly.

e. The Oversight Committee shall address any requests or feedback received, respond to and resolve the issue within thirty (30) days.

f. This Article does not prohibit a data subject from seeking legal redress under the Country legal system.

Part Four: Technical Measures

12. Technology

a. The technology to be adopted for the purpose of data stewardship initiatives shall be configured in such a way to ensure –

i. interoperability to facilitate data sharing for the purposes described in Schedule C,

ii. collective ownership of data, including the potential for data subjects to assert their rights,
iii. compliance with cyber security and data protection by design and by default principles, and
iv. use of appropriate industry standards in encryption, pseudonymisation, and anonymisation.

b. The Data Steward, with advice from the Oversight Committee, shall advise on the appropriate technology to be adopted in data stewardship initiatives, both by the Data Host and the Members.

c. The final decision regarding which technology to use, and how that technology should be used (including security measures), both collectively and individually, shall rest with the Members themselves.

d. The Oversight Committee shall periodically carry out industry standard risk and impact assessments of the technology used for data stewardship initiatives and submit the report to the Data Steward for consideration.

13. Data subject access

a. In consultation with the Data Steward, the Data Host shall provide data subjects with access to their data, providing an overview of:

i. any of their personal data which is being held by the Data Host,
ii. any data about the assistance which Members are providing them.

14. Data Sharing

a. The Oversight Committee shall every twelve months review the list of data points to be shared by Members for purposes of data stewardship initiatives.

b. The Data Steward with advice from the Oversight Committee shall give direction on the format of data to be adopted in data stewardship initiatives.

c. Members shall agree a format to share data that is machine readable and facilitates interoperability between the Members and the Data Host.

d. The Data Host shall maintain reference versions of any data standards adopted by the Data Steward, and a catalogue of data shared by Members.

15. Data Security

a. Only authorised persons shall have access to data held by the data stewardship initiatives under this Framework.

b. The Data Host shall maintain a register of authorised persons, both on the platform and separately.

c. Appropriate measures shall be undertaken by all Members to ensure that no unauthorised persons access alter or destroy data.

d. In case of a confirmed security or data breach, the Data Host shall notify the Oversight Committee within one (1) Business Day.

e. The Oversight Committee shall constitute an *ad hoc* Committee to address a confirmed security or data breach.

f. The Data Host and Oversight Committee shall comply with security and data breach reporting regulations of the Country .

16. Data Retention

a. Data shall be retained by the Data Host for a period or periods agreed upon in advance by the Data Steward.

b. The Data Host shall be responsible for implementing data retention and deletion policies with the agreement of the Data Steward.

c. Upon deletion, the Data Host will inform the Members who originally contributed that data to the Steward that the data has been deleted.

17. Third Party Access to Data[13]

[13] If the Data Steward believes that any data sharing with any third parties would not be appropriate, this section can be removed. The section can also be amended to specify a) which types of third party and b) which types of data can be considered for data sharing in order to mitigate potential risks.

a. A third party may request access to data held by the Data Steward by a written request to the Oversight Committee which states the specific purpose for which the data will be used.[14]

b. A request shall only be considered if the stated purpose of the request is to improve service provision to affected populations, and if the third party is considered by the Oversight Committee to align with the principles underlying this Framework.

c. The Oversight Committee has the authority to approve or deny any request, but should seek advice from the Data Host and/or the Members as necessary to ensure that the data will be used appropriately and in a secure manner.

d. A request for access will be granted only

    a. once the third party signs the Data Sharing Agreement which should accompany this Framework, and
    b. with written approval from the Oversight Committee communicated to the Data Host.

e. Any third party granted access who then violates the provisions of the Data Sharing Agreement, uses the data to which they have been granted access for any purpose other than the specific purpose approved by the Oversight Committee, or otherwise violates the principles underlying this Framework, shall have their access revoked immediately.[15]

f. There shall be a register of all third parties who are granted access to data maintained by the Data Host.

[14] Situations in which data sharing with a third party should be considered on a case-by-case basis. Examples might include: researchers analysing the data to help the Members to improve their service delivery; a government agency reviewing the data as part of a transition to a social protection scheme; or a private company engaged in service delivery on behalf of the Members.

[15] While there is no provision for legal action included in this document, the Data Steward may wish to consider how they would respond in the event of a breach of this section by a third party, whether through legal means or other avenues.

18. Implementation[16]

Implementation of this Framework shall be as set out in Schedule A. The Schedule may be amended at any time by a majority vote of all Members.

[16] The Framework should be implemented progressively. This means that not all aspects of the Framework need to be introduced immediately, or at the same time. Members should decide on a timeframe which is appropriate for the environment in which they are working, and the capacity which they possess both individually and collectively.

Part Five: Signatures[17]

In WITNESS WHEREOF, the parties below have executed this Framework

Organisation:

Registered Address

Name:

Position:

Contact Email:

Signature:

Date:

Organisation:

Registered Address

Name:

Position:

Contact Email:

Signature:

Date:

[17] The Governance Framework does not specify a resource commitment by the Signatory Organisations, but since there is a) commitment of staff time, and b) legal implications regarding data management, the Signatory should be a staff member empowered to sign contracts on behalf of the Organisation.

Organisation: Registered Address: Name: Position: Contact Email: Signature: Date:
Add signatories as needed.

Schedule A: Implementation Timeline[18]

The timelines under this Schedule shall apply from the date on which three founding organisations sign this Framework.[19] The status of founding organisation does not confer any special privileges within the Data Steward or any subsidiary body.

Timeline	**Activity**
Within three months	● Set up the Data Steward. ● Designate the Data Host. ● Agree the Data Standard(s). ● Agree Standard Operating Procedures. Note: During this period, the Data Steward may also act as the Oversight Committee.
Within six months	● Incorporate representatives of data subjects or affected populations into Data Steward. ● Establish appropriate complaints (or other feedback) mechanism into Data Steward. Note: During this period, the Data Steward may also act as the Oversight Committee.
Within 12 months	● Set up the Oversight Committee as and when more than ____ organisations sign up to the Framework. ● Review the Framework to ensure it is meeting the needs of Members and beneficiaries.
Within 24 months	● Fully operationalise the Framework

[18] This timeline should be adjusted depending on the intentions and capabilities of the founding organisations. It should take into account the amount of time that will be needed to achieve each step, especially if it is envisaged that other organisations will join the Data Steward during the timeline.

[19] The number of founding organisations required to commence implementation can be adjusted depending on how many founding organisations there are, but also on the size and scope of the Data Steward itself. For example, if all the founding organisations sign the Framework separately over a period of weeks, implementation should not start until that threshold is reached.

Schedule B: Focal Points for each Member Organisation

Each organisation should identify a Focal Point for the activities of the Data Steward within that organisation.[20]

The Focal Point will be responsible for implementation of the Data Steward within their organisation, including identifying other staff who may take on specific roles for specific activities.

Each Focal Point should be identified by name and position, and a contact email provided, in the spaces below.

Organisation	Name	Position	Email

[20] The focal point may or may not be the same person who is assigned by the organisation to the Data Steward as a Representative, either to the Oversight Committee or to any other body formed by the Data Steward. The focal point may not be the same individual as the signatory, but even if they are the same individual they should be listed in the Schedule.

Schedule C: Overall and Specific Purposes of the Governance Framework

This Schedule contains a description of the Overall Purpose for which the Framework has been concluded.[21] This Purpose will consist of one or more specific purposes, each of which is listed and described below.

A description should include a general description of the use case which is being addressed by the purpose, as well as the specific data and metadata that will be shared to achieve that purpose.[22]

This list may be amended by written agreement of all Members either to remove or to add a Purpose. Should Members agree to add a Purpose to the list, a description of that Purpose must be included.

If a list of purposes is already included in the Data Sharing Agreement which should accompany this document, then the list of purposes in that DSA may also be appended to this Framework as Schedule C.

Overall Purpose

Members of the consortium will share Shared Information (as defined herein) with the designated Data Host at a country consortium level of programming participants of projects jointly implemented by consortium members in order to achieve the specific purposes listed below.[23]

Specific Purpose(s)

The list of data and metadata must provide an exhaustive list of all personal information to be shared between the Parties (for example, name, address, sex, phone number, ethnicity, etc.).

If new Personal Information is to be shared after this Agreement is signed, this Schedule must be amended. High-Risk Personal Information should be explicitly identified as such.

Common purposes for interoperability are given below. Any other purposes agreed upon by the Data Steward may be added to this list.

[21] A sample text of an Overall Purpose is included in this template, which should be replaced by the Parties.
[22] Two examples of such use cases are included in this template, and further use cases may be added at a later date.
[23] Where the Agreement is concluded in order to contribute to the achievement of a specific funded project or projects, a short text may be included here which describes that project.

Purpose 1

Title	Deduplication of persons
Description	
Data	
Metadata	
Notes	We are deduplicating individuals not households.

Purpose 2

Title	Deduplication of assistance
Description	
Data	
Metadata	
Notes	We are deduplicating individuals not households.

Purpose 3

Title	Referral of individuals
Description	Organisations providing cash assistance may sometimes encounter individuals or households with specific needs that are not currently being met, and which the organisation cannot meet. In these situations member organisations may need to refer

	individuals to another organisation which provides services which can meet those specific needs.
Data	
Metadata	
Notes	

Purpose 4: Beneficiary Data View

Annex A: Principles for Data Responsibility in Humanitarian Action[24]

This Framework is guided by the Principles for Data Responsibility in Humanitarian Action, developed and endorsed for IASC Operational Guidance on Data Responsibility of April 2023.[25] This Annex contains a complete description of those principles.

Accountability

In accordance with relevant applicable rules, humanitarian organizations have an obligation to accept responsibility and be accountable for their data management activities. Humanitarian organizations are accountable to affected populations, to internal governance structures, and to national, regional and international actors and authorities, as applicable. Humanitarian organizations should put in place all measures required to achieve their accountability commitments in line with these Principles. Such measures include establishing adequate policies, guidance, and processes, and ensuring that sufficient and appropriate competencies and capacities are available, including but not limited to financial, human and technological resources.16 Establishing competencies and capacities should include offering training and learning opportunities to ensure that staff have the expertise, skills, knowledge and attitudes needed to manage data responsibly

Confidentiality

Humanitarian organizations should implement appropriate organizational safeguards and procedures to keep sensitive data confidential at all times, including through clear and consistent access restrictions. Measures should be in line with applicable organizational policies and legal requirements, while taking into account the relevant data and information sensitivity classification system(s) in the response context.

Coordination and Collaboration

Coordinated and collaborative data management entails the meaningful inclusion of humanitarian partners, national and local authorities, people affected by crisis, and other stakeholders in data management activities, where appropriate and without compromising the humanitarian principles17 or this Operational Guidance. Humanitarian organizations should coordinate and collaborate to ensure that appropriate connections are established between humanitarian operational data management activities and longer-term development-oriented data processes and data investments. Local and national capacity should be strengthened wherever possible, and not be undermined.

Data Security

Humanitarian organizations should implement appropriate organizational and technical safeguards, procedures and systems to prevent, mitigate, report and respond to security breaches of both digital and non-digital data. 18 These measures should be designed to protect against material external breaches as well as unauthorized or inappropriate internal access or manipulation, accidental disclosure, damage, alteration, loss, and other security risks related to data management. Measures should be based on the sensitivity of the data and updated as data security standards and best practice evolve.

---

[24] The Data Steward may choose not to append this Annex to the Framework Document, and refer directly to the Operational Guidance. We include it as a reference for readers who may not be aware of that Guidance.

[25] The full text of the Operational Guidance is available at https://interagencystandingcommittee.org/operational-response/iasc-operational-guidance-data-responsibility-humanitarian-action.

Defined Purpose, Necessity and Proportionality

Humanitarian data management and its related activities should have a clearly defined purpose. The design of processes and systems for data management should contribute to improved humanitarian outcomes, be consistent with relevant mandates, respect and promote rights and freedoms, and carefully balance those where needed. In line with the concept of data minimization, the management of data in humanitarian response should be relevant, limited and proportionate to the specified purpose(s).

Fairness and Legitimacy

Humanitarian organizations should manage data in a fair and legitimate manner. Fair data management enables the delivery of humanitarian action in a neutral and impartial manner. Legitimate grounds for data management include, for example: the best and/or vital interests of communities and individuals affected by crisis, consistent with the organization's mandate; public interest in furtherance of the organization's mandate; and any other legitimate ground specifically identified by an organization's regulatory framework and/or applicable laws.

Human Rights-Based Approach

Data management should be designed and implemented in ways that respect, protect and promote the fulfillment of human rights, including fundamental freedoms and the principles of equality and non-discrimination as defined in human rights frameworks, as well as data-specific rights promulgated in applicable legislation.

People-Centered and Inclusive

Affected populations should be afforded an opportunity to participate and be included, represented, and empowered to exercise agency in all steps of data management for a given activity, whenever the operational context permits. The human autonomy of people affected by crisis should guide humanitarian data management. Special efforts should be made to support the participation and engagement of people who are not well represented or may be marginalized in a given data management activity (e.g., due to age, gender and other diversity characteristics such as disability, ethnicity, religion or sexual orientation), or are otherwise 'invisible', consistent with commitments to leave no one behind. These should include fostering data literacy across and within communities.

Personal Data Protection

When managing personal data, humanitarian organizations have an obligation to adhere to (i) applicable national and regional data protection laws, or (ii) if they enjoy privileges and immunities such that national and regional laws do not apply to them, to their own data protection policies. These laws and policies contain the principles for personal data protection, such as a list of equally valid legal bases for the processing of personal data, including but not limited to consent. Humanitarian organizations subject to national or regional legislation should also take into account the guidelines and advisories issued by relevant data protection authorities within their applicable jurisdiction. When designing data management systems, humanitarian organizations should meet the standards of privacy and data protection by design and by default. Humanitarian organizations should take personal data protection into consideration when developing open data frameworks. In line with their commitment to ensure accountability to affected people, inclusivity and respect for human rights, humanitarian organizations should uphold data subjects' rights to be informed, in an easily accessible and appropriate manner, about the processing of their personal data, to be able to request to access, correct, delete, object to or request information about the processing of their personal data, and to not be subject to automated

decision-making except under the specific conditions set out in the legal frameworks applicable to an organization.

Quality

Data quality should be maintained such that the owners, users and other key stakeholders are able to trust data management activities and their resulting products. Data quality entails that data is relevant, accurate, timely, complete, standardized, interoperable, well-documented, up-to-date and interpretable, in line with the intended use and bearing in mind the given operational context. Where feasible and appropriate, and without compromising these Principles, organizations should strive to collect and analyze data by age, sex and disability disaggregation, as well as by other diversity characteristics as relevant to the defined purpose(s) of an activity.

Retention and Destruction

Organizations should establish a data retention and destruction schedule that indicates how long data will be retained and when data should be destroyed, as well as how to do so in a way that renders data retrieval impossible. Sensitive data should only be retained for as long as it is necessary to the specified purpose(s) for which it is managed or as required by applicable laws or audit regulations. When retaining sensitive data, organizations should specify and ensure its safe and secure storage to prevent misuse or exposure. Non-sensitive data may be retained indefinitely, in line with applicable laws, regulations and policies, and provided that access rights are established and the sensitivity of the data is reassessed on a regular basis.

Transparency

Organizations should manage data in ways that offer meaningful transparency toward humanitarian actors and stakeholders, particularly affected populations. This should include the provision of timely and accurate information about the data management activity such as its purpose(s), the intended use(s) of and approaches to sharing the data, as well as any associated limitations and risks.