Working draft v1 - February 2025

Prepared by the Data Responsibility Working Group - not reviewed or endorsed by all members

Data Responsibility in Rapid Scale-Down or Closure of Operations

Loss and exposure of operational data are critical risks that often go unaddressed during rapid scale down or closure of operations. Loss of operational data can impact the ability to effectively plan, prioritize, respond, monitor and report, as well as the ability to undertake evidence-informed advocacy and resource mobilization. Exposure of sensitive data can lead to harm to affected people, host communities and humanitarian personnel, and can impede humanitarian organizations in their response.

Organizations scaling down or phasing out operations involving humanitarian data management must decide how operational data - including sensitive data and personal data - will be managed. These decisions should avoid doing harm and be based on organizational policies - including policies on data protection, security, retention and archiving. The decisions should be guided by the principles for data responsibility, using people-centered approaches that focus on the maximisation of benefits and the minimization of risks. More specifically, these decisions should aim to:

1. Avoid the exposure of personal data and sensitive non-personal data
2. Safeguard the continued availability of data, based on a defined and specific purpose
3. Understand the impact on other operations or programmes
4. Inform partners of changes in data quality, availability and access
5. Inform data subjects of transfer, retention or destruction of their personal data.

Personal data should always be managed in line with applicable organizational policies and legislation. Consult legal, information security or data protection focal points to help decide on data retention, transfer or destruction and to navigate applicable data localisation and data protection requirements.

The Data Responsibility Working Group (DRWG) has prepared the following checklist for situations of rapid scale-down or closure of operations, based on the IASC Operational Guidance on Data Responsibility in Humanitarian Action. This checklist aims to help inform decisions about whether to retain data internally for future use, publish it on external platforms, transfer it to a third-party, or destroy it:

1. **Map what data is being managed in the operation**
   Develop an overview of data management activities in the operation, e.g. a data management registry. This overview should indicate the activities for which personal data is being processed.

2. **Assess the operational relevance**
   Review the data managed in the operation and determine what data is relevant to the work of your organization or partners. For example, data may be needed internally for operational continuity or for audit purposes, shared for use by specific partners, or publicly shared for general use in support of overall humanitarian response.

3. **Assess data sensitivity**
   Consider the likelihood and impact of harm to affected people, host communities and humanitarian personnel in case of accidental or intentional exposure of the data, as well as the potential impact on the organization and partners. If available, review the Information Sharing Protocol for the response context to determine the sensitivity level.

4. **Assess internal capacity to retain data and safeguard continued data availability**
   Identify the availability of secure and sustainable storage or archiving modalities within your organization, noting these should be appropriate to the sensitivity level of the data. Review access permissions to prevent unauthorized access to data and systems and the ability to revoke access, and ensure the continued availability of data to those who need it for a specific purpose.

5. **Assess partner capacity to responsibly receive, store, and manage data**
   Determine whether partners may be in a position to take over management of relevant data, including its secure reception and storage.

6. **Based on steps 1 - 5, decide for each data management activity whether data should be retained, published, transferred, or destroyed.**

    a. **Retention**
       If the data is operationally relevant and you have the appropriate infrastructure available to securely maintain it, consider data retention. Set an initial retention period and determine the geographical location of storage (as relevant). Identify storage infrastructure and put in place appropriate security measures and data access permissions.

    b. **Publication**
       If the data is operationally relevant, but it is difficult for you to maintain access, consider publishing it on an external platform. Useful non-sensitive data can be published through platforms such as HDX or Reliefweb to ensure its continued availability.

c. **Transfer**
If the data can be used by a partner to maintain operational continuity, consider transferring it to one or multiple partners. Before transferring sensitive data, determine whether secure channels are available to share the data, whether data sharing agreements are in place if needed, and whether partners have the capacity to securely manage the data.

d. **Destruction**
If the risks of data retention, publication or transfer outweigh the benefits, consider destruction. Consult applicable organizational policies on archival and retention before destroying data, and consider creating an aggregated version that can be retained, published or transferred. Ensure there is a clear rationale for data destruction and document the rationale, and use a tool that renders data retrieval impossible.

7. **Communication with affected people**
When communicating on the scale-down or closure of operations to affected people, include a notice on what will happen to personal data wherever possible. E.g. “data collected as part of this project will be retained for 3 years from the moment of suspension of the project” or “data related to this project will be destroyed and will not be shared outside our organization”. Wherever feasible, affected people should be given the opportunity to request deletion of their personal data, in-line with applicable organizational policies or legislation.

Contact the Data Responsibility Working Group to reach out to other humanitarian organizations for best practices on data responsibility in the context of rapid scale-down or closure of operations.