



Purpose:

Including data responsibility considerations in the design, implementation, monitoring and evaluation of data management activities led by the working group helps minimize risks and maximize benefits.

OCHA's Role:

OCHA and the Co-Leads should ensure that data management activities led by the working group are designed for data responsibility, including by developing relevant standard operating procedures (SOPs).

Recommended Approach:

- ☐ Working groups should incorporate data responsibility, including data protection and privacy, into data management by design when planning any data management activity.
- ☐ Designing for data responsibility includes, for example, the following steps and considerations:
 - Establish clear and replicable SOPs for data management activities. The IASC Operational Guidance includes a template SOP. SOPs should include information regarding applicable data subject rights where personal data is processed, and should specify the channels for requests regarding these rights.
 - When selecting tools for data management, foster complementarity, interoperability (where appropriate, including with governmental and other local systems), and harmonization (including on terminology, typologies and data structure).
 - Ensure the working group has assessed risks associated with any use of emerging technologies, including artificial intelligence, blockchain or other similar tools to process data or produce analysis.
 - Offer training to working group members and partners on responsible data management, including on guidance developed by the working group for its data management activities.
 - Support measures for the safe management of data (e.g., for data anonymization, provision of secure storage and data transfer solutions, etc.).
 - Adhere to relevant guidance and protocols on data responsibility and related processes and procedures, including ISPs. This includes ensuring all data that needs to be shared for defined purposes is made available through appropriate channels in a responsible manner, with the necessary safeguards for personal data and in compliance with applicable data protection frameworks.