02 CREATE AND MAINTAIN A DATA MANAGEMENT REGISTRY FOR THE OFFICE

Purpose:

OCHA offices should establish a data management registry to track all data management activities they are leading or contributing to. Some data management activities may already be included in tools such as a survey of surveys or an assessment registry. OCHA personnel should consult the registry and any similar tools before undertaking any new data collection in order to avoid duplication.

Policy Requirement:

- ☐ While the tracking of all data management activities is recommended, OCHA offices must record activities involving the management of personal data and 'non-personal data in a sensitive context'. The record of such activities must specify the purposes and means of the processing, the content and use of the data being processed, and any mitigation measures in place.
- ☐ The registry capturing these details must be shared with the data protection focal point to support the 'data mapping' mandated by the UN Secretariat Data Protection and Privacy Policy.

Recommended Approach:

- ☐ The IM unit in the OCHA office is responsible for developing a data management registry for all data management activities by the office. All staff involved in data management should be aware of the registry and know how to update it.
- ☐ The data management registry must at a minimum include the name, type, timeframe and actors involved in the data management activity, as well as the tools and infrastructure used, applicable guidance such as SOPs and ToRs for the activity, requirements for onward data sharing, and data retention and destruction timelines in line with applicable instructions from the data protection focal point.[16]
- ☐ The IM unit should share the data management registry with the data protection focal point.

Relevant Tool or Template:

IASC Data Management Registry Template

[16] According to the UN Secretariat Data Protection and Privacy policy, data stewards will establish internal processes in their respective entities for the periodic deletion of personal data and non-personal data in a sensitive context that is no longer needed for any purpose that is consistent with a legal basis for data processing.