Data Responsibility Policy

Rationale behind this policy

[Organizations rationale]

Purpose of the policy

[Organizations purpose]

Attribution

You can use this policy for non-commercial purpose and as a base for adapting your own policy, but please be so kind to give us some credit and reference it by indicating the following sentence where appropriate:

Please note that we used the data responsibility policy as initially developed and drafted upon initiative of the Netherlands Red Cross - *510 as a source of inspiration and starting point for the adaptation of our own policy, for the content and performance of which we carry sole responsibility.*

Date of change of the policy Version 3.1: 20 April 2018

1. Objective

The objective of this policy is to form the basis for how to handle data within the work context of [the organization]. It establishes principles that guide the responsible use of data and processes that help ensure its application.

2. Scope

This policy applies to all data used in the work of [the organization], whether within the team, in cooperation with other teams of [the organization], or together with third parties. All team members of [the organization] need to comply with the policy irrespective of the physical location where they carry out their tasks.

3. Target audience

This policy serves as a reference to all staff members. In 510 we typically identify the following roles in data projects:

Data curator: A team member tasked with exploring, updating and storing open datasets, metadata information and other relevant documents in a well-structured central database or repository system, ensuring that the most current datasets are easily searchable and accessible for analyses. This role is sometimes referred to as “data steward” or “data manager”.

Data owner: Single-point-of-contacts in a team tasked with keeping track of any legal documents such as Non-Disclosure Agreements (NDAs), Memorandum of Understanding (MoU), commercial contracts, or other forms of communications in which they were involved. These documents may be required as part of receiving or purchasing the required data from third parties, or when sharing data with others.

Data analyst: A team member tasked with exploring, processing, analysing and/or visualizing data, which is specifically non-Personal Data, non-Personally Identifiable Information, or non-Demographically Identifiable Information. If the data is Personal Data, PII or DII, the role is called Data processor.

Data processor: Identical to the role of Data analyst, except the data is now of the type Personal Data, PII or DII. This role is explicitly mentioned in the General Data Protection Regulation (GDPR).

Data controller: A team member tasked with determining the purpose and means for processing data of the type Personal Data, PII or DII. This role is explicitly mentioned in the GDPR.

Data project lead: A team member tasked with managing a project team, ensuring a timely delivery of a data project within a specified budget, for which the deliverables are of an agreed quality level.

Data team lead: A reserved role within a data team, tasked with sign-offs at start and closure of data projects, risk assessment and evaluation of contingency measures, etc.

IT: A team member tasked with providing expertise in maintaining a data storage network, applying software upgrades to ensure data protection.

An overview of how these roles relate to each other is presented in the chapter on the data life cycle.

4. Definitions

For this policy the following terms and definitions are applicable:

a. Personal Data & Personally Identifiable Information (PII)

Personal Data and Personally Identifiable Information is any information relating to an identified or identifiable natural person, who can be identified, directly or indirectly, by means reasonably likely to be used related to that data. This includes cases where an individual can be identified from linking the data to other data or information reasonably available in any form or medium.

Publicly available data can also be personal.

Examples:

- Biographical data such as: name, sex, marital status, date and place of birth, country of origin, age, address, telephone number, identification number, etc.
- Biometric data such as: a photograph, fingerprint, facial or iris image, DNA, etc.
- Online identifiers such as your unique laptop number or IP-address.

What constitutes personally identifiable data is continually expanding, as technological advancements make it possible or easier to derive an individual's identity using disparate pieces of information from the wide range of datasets that are now accessible. Therefore, the list of examples is merely meant to provide users with a better understanding of the definition and is by no means exhaustive.

b. **Demographically Identifiable Information (DII)**[1]

Demographically Identifiable Information is data that can be used to identify a community or distinct group, whether geographic, ethnic, religious, economic, or political.

c. **Data Subject**

The data subject is a natural person (i.e. an individual) who can be identified, directly or indirectly, in particular by reference to Personal Data.

d. **(Informed) Consent**

(Informed) consent is any freely-given, specific and informed indication of agreement by the Data Subject to the collection and processing of Personal Data relating to him or her. This agreement may be given either by a written or oral statement or by a clear affirmative action. One should note that agreeing to a disclaimer or using data under a license can be a clear affirmative action.

e. **Data Controller**

The data controller is any team member who, alone or jointly with others, determines the purposes and means for the processing of Personal Data or Personally Identifiable Information, or Demographically Identifiable Information.

f. **Data Processor**

A data processor is any natural person or organization that carries out processing of Personal Data, Personally Identifiable Information, or Demographically Identifiable Information on behalf of the Data Controller.

g. **Third Party**

A Third Party is any natural or legal person, public authority, agency or body other than the Data Subject, Controller, or Processor.

Examples:

- National governments
- International governmental or non-governmental organisations

[1] Interchangeably, the common term Community Identifiable Information (CII) is used.

- Private sector entities or individuals, such as: consultants, agencies providing online services for storing personal data, etc.

5. Principles

The policy is built upon the following principles of data responsibility:

a. Purpose specification

The collection and use of data for a specific dataset shall be guided by a pre-defined, practical and precise purpose. Data shall not be further processed in any manner that is incompatible with the specific purpose. It shall be clearly outlined how the purpose serves a humanitarian end.

b. Respect for the rights of the data subject

The use of data shall be guided by respect for the rights of the data subject, such as dignity, informed consent, and not to be put at risk through the collection and use of data. Everyone has a right to privacy, including data regarding PII and DII and the protection thereof.

All reasonable efforts shall be undertaken to obtain informed consent from the data subjects to use personal data for the purpose of the project. This data cannot be re-used for other purposes than the consent was given for.

Data subject's personal data will be destroyed after it has served its stated purpose. The GDPR (http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf) identifies three exceptions to this: the data is needed to (a) exercise the right of freedom of expression, (b) there is a legal obligation to keep the data or (c) there are reasons of public interest.

c. Do no harm

The basic principle is that all reasonable measures shall be taken to avoid causing any harm. This means considering the context of the project, including political and cultural sensitivities. It aligns with humanitarian principles. If the use of any data may pose significant risks to any concerned party, one shall refrain from executing the project. This will require an ethical review of the project before initiation and monitoring during execution.

d. **Necessity and proportionality**

The data should be necessary to achieve the purpose. The data collection should be proportionate with regards to the envisioned humanitarian benefits and the potential for harm. This means, amongst others, that data minimisation and destruction of personal data after a specific time period need to be applied, in accordance with protocols agreed upon in conjunction with the purpose of data collection and use.

e. **Legitimate, lawful and fair use**

Data shall be collected and used in such a way as to not infringe upon the legitimacy of the [organization]

This means that access and use of the data has to be in accordance with applicable law as well as respecting terms and conditions of data providers. Explicit written permission is required from third party data providers when planning to use data for any other reason than foreseen according to their terms and conditions.

When obtaining data from third parties or in collaboration with third parties, or when sharing data with authorized partners or third parties, all reasonable efforts need to be made that the principles of impartiality and neutrality are upheld. In this context, impartiality means specifically that none of the data can and must be used to discriminate against individuals and groups. Neutrality means that data and insights must not be used for political or economic interest.

Data which contains PII and/or DII shall not be provided to third parties, unless this is specifically agreed upon in the informed consent and the third party is disclosed to the data subject.

f. **Data security**

In order to prevent potential loss or harm, reasonable administrative and technical security measures and privacy by design processes shall be in place and observed.

g. **Data quality**

The data shall be as adequate, accurate, up to date, valid, reliable and relevant as possible for the specific purpose.

5. Operational Guidance

This section provides practical guidance on how to apply the principles.

1. Purpose statement

The very first step is to specify the purpose statement for the project. This is a pre-defined, practical and precise purpose. It should be articulated carefully because the purpose statement will deeply affect the project, especially if personal data is involved, in the following ways:

- Personally Identifiable Information shall not be further processed in any manner that is incompatible with the specific purpose.
- Data shall only be shared with third parties if it is going to be used for the same purpose.
- Once the purpose has been served, any personally identifiable information must be destroyed (see 5b for exceptions).

2. Type of data

The second step is to determine what type of data will be collected, processed or published as part of specific deliverables of your project. This policy distinguishes the following types of data with different levels of sensitivity:

- Personally Identifiable Information (PII):

  Any information that can lead to the identification, directly or indirectly, of a natural person.

- Demographically Identifiable Information (DII)

  Any information that can be used to identify a community or distinct group, whether geographic, ethnic, religious, economic or political.

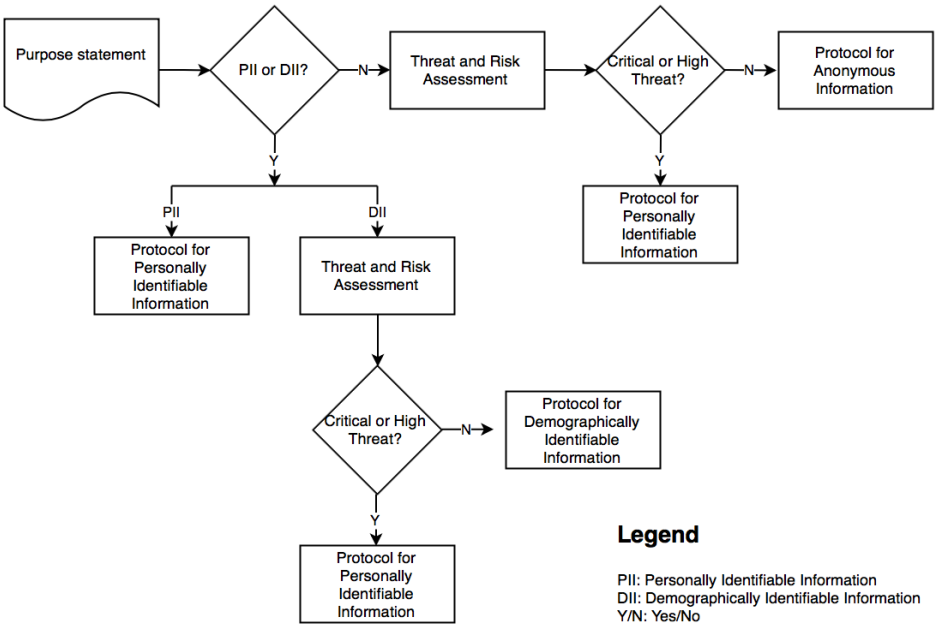
- Anonymous Information (AI):

  Information that ***cannot*** be used to identify individuals or groups, directly or indirectly. PII or DII can be ***anonymised*** and become anonymous information, provided the raw/unprocessed information has been deleted from all storage locations

A protocol exists for each type of information, with increasing requirements in terms of security and protection. Data ***responsibility*** means that when you work with any data, including anonymous data, you should reflect on whether the data you work with could

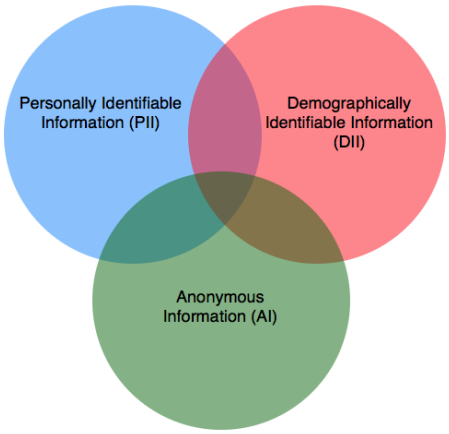
be used to harm or otherwise disadvantage other people. To assess the potential for harm you should make a ***threat and risk assessment*** (see annex) at this point of project design and again at any other point during the project's implementation that you consider this to be relevant. ***In case a critical or high risk is identified, you should do the following:***

1. Apply the protocol for PII.
2. Determine what additional mitigation strategies can be applied or developed to execute the project in a responsible way.
3. In case no suitable mitigation strategies can be identified, determine whether the project should be aborted.



– <u>Multiple types of data</u>

Your project may involve multiple types of data as visualised in the Venn diagram below. You may opt to apply the protocol for the most sensitive type of information to the entire dataset or, if there is a need for you to keep part of your information under a less strict regime, you may opt to maintain two or more datasets governed by different regimes[1]. This will imply additional work and costs.



3. Data collection

The third step after articulating the purpose statement and determining what type of data you are going to work with, is to work out ***how*** you are going to go about collecting the data you need. There are minimum risk prevention measures that should be applied in all cases and different data protocols that should be applied depending on the type of data that you have determined you will be working with.

I. Minimum risk prevention measures

When initiating the project:

a. Complete the checklist and obtain approval for your project proposal. (see annex)
b. ***Obtain local knowledge***. For this you should engage a local (Red Cross/Crescent National Society) expert or other relevant local partner of the country, who is knowledgeable in the area of (data) policies and risks in the contextual setting of that country.
c. Check the applicable legal framework to ensure that you have a legal basis for accessing and collecting the data.
d. Verify if any additional rules or restrictions apply to your data source(s):
    i. Evaluate the timeliness of the dataset by checking when the data was released
    ii. Check any terms, conditions and licenses of third party data providers. Note: copyright legislation differs from country to country.
    iii. Check for any licenses associated with your data, which indicate the data ownership and the conditions under which the data may or may not be used.
    iv. Check if you need to acquire a written copyright permission from the content owner.
    v. Check if it is necessary to obtain an exception to use copyrighted materials for purposes other than those provided for (e.g. in the disclaimer).

vi. Record any licences or permissions with the datasets they pertain to.

e. In all instances you should aim for ***data minimisation***: only collect data that is necessary for the pre-defined purpose of the project as well as proportionate and not excessive in scope.
f. Log the dataset's relevant metadata in an appropriate system.
g. Apply a ***dataset*** sensitivity classification as part of the dataset's metadata (see annex).
h. Apply a ***document*** sensitivity classification on the first page or in the footer (see annex).
i. Use the third-party data sharing agreement template (see annex) in any situations in which you share (provide or receive) data with third parties.
j. Ensure that any published maps or dashboards containing boundary data have been accompanied by the following disclaimer: "The *maps used do not imply the expression of any opinion on the part of the Red Cross and Red Crescent Movement concerning the legal status of a territory or of its authorities"*. (see annex)
k. Prior to publication (e.g. via a website or any other media channels), any communications about a project, or its products, must undergo a technical review in which the minimum risk prevention measures are evaluated.
l. After publication, data shared through online platforms should come with a proper data sharing licence. The data sharing platform should restrict indexing and caching of datasets.

<u>During implementation of the project/at mid-term:</u>

a. Ensure the relevance of the dataset continues to be in line with the stated purpose of using the data.
b. Evaluate the accuracy of the dataset e.g. in terms of completeness and any errors in the (personal) data.
c. Correct the errors in the (personal) data.
d. Evaluate the interpretability of the dataset by checking for completeness and clarity of the dataset
e. If relevant, evaluate the comparability of the dataset by comparing the dataset with similar or related datasets in terms of coherence of data.
f. If possible, remove the personal data from the dataset and check the quality items.
g. Regularly review the dataset and document sensitivity classifications and the storage options.

<u>When closing the project:</u>

a. Prepare an internal project evaluation between the project team and involved stakeholders to identify and share any best practices, bad practices and possibilities for improvement.
b. Centrally archive and retain documentation such as signed contracts, copyright permissions, and final reports as long as deemed necessary.
c. Archive all permissions and approvals.
d. Obtain confirmation from all third-party storage providers that any personal data was successfully removed after closure of the project.
e. Ensure that any personal data and its metadata are destroyed from all storage locations.
m. Ensure that your final reports address the research methodology applied in the project, as well as the data sources and metadata used.

II. Protocol for working with Personally Identifiable Information

If you collect, process or publish personal data or personally identifiable information you need to proceed as follows:

1. Respect for the rights of the data subject:
    a. Obtain informed consent from the data subject(s) to use their personal data for the purpose of the project. In case a data subject is under 16 years of age, as per the GDPR parental consent must be obtained. When obtaining consent, each data subject must be informed of the following:
        i. The purpose of the data collection.
        ii. The existence of a mechanism that allows data subjects to verify their personal data, request information on how their data is being handled, to withdraw consent and to have personal data corrected or deleted.
        iii. The guarantee that the personal data they provide is not re-used for other purposes than the consent was given for.
        iv. In case data subjects withdraw their consent, or object to processing of their personal data, they are informed about a successful destruction of their personal data.
        v. That their personal data will be destroyed after the project closes and/or after a specified time period ***unless*** the data is needed to (a) exercise the right of freedom of expression, (b) there is a legal obligation to keep the data or (c) there are reasons of public interest.
2. Do no harm:
    a. Products produced by [the organization], I.e. maps, online dashboards, infographics or other forms of information shall not be shared publicly if

they contain personal data/personally identifiable information of individuals or pose a significant[2] risk to groups of individuals.

3. Data security/IT system requirements:
    a. Record the consent statement with each data record for future reference.
    b. Apply "privacy by design" principles to each phase of the project from initiation to archival procedures. (see annex)
    c. Set the time period for the destruction of personal data in conjunction with the purpose of data collection and use.
    d. Enable finding and destroying single data records without affecting the quality of the overall data set.
    e. Apply user permission policies associated with a dataset sensitivity classification (e.g. reading permissions, editing permissions, full control). (see annex)
    f. Apply user permission policies associated with a document sensitivity classification (e.g. reading permissions, editing permissions, full control). (see annex)
    g. Employ appropriate and reasonable technical and administrative safeguards (e.g. strong security procedures, de-identification of data) depending on the level of classification.

III. Protocol for working with Demographically Identifiable Information

If you collect, process or publish demographically identifiable information you need to proceed as follows:

1. Do no harm:
    a. When collecting, processing and using data, ensure that DII cannot be used to put groups and individuals at risk. Conduct a threat and risk assessment. (see annex)
    b. Do not publicly share any maps, online dashboards, infographics, other forms of information, etc. if they contain personal data/personally identifiable information of individuals or pose a significant risk to groups of individuals.

2. Data security/IT requirements:
    a. Apply "privacy by design" principles to each phase of the project from initiation to archival procedures.

[2] A "significant" risk constitutes any identified risk higher than "low risk" as per the Threat and Risk Assessment guidelines. (see annex)

b. Employ appropriate and reasonable technical and administrative safeguards (e.g. strong security procedures, de-identification of data) depending on the level of classification.
c. Apply user permission policies associated with a dataset sensitivity classification (e.g. reading permissions, editing permissions, full control).
d. Apply user permission policies associated with a document sensitivity classification (e.g. reading permissions, editing permissions, full control).
e. Regularly review the dataset and document sensitivity classification and the storage options.

IV. Protocol for working with Anonymous Information

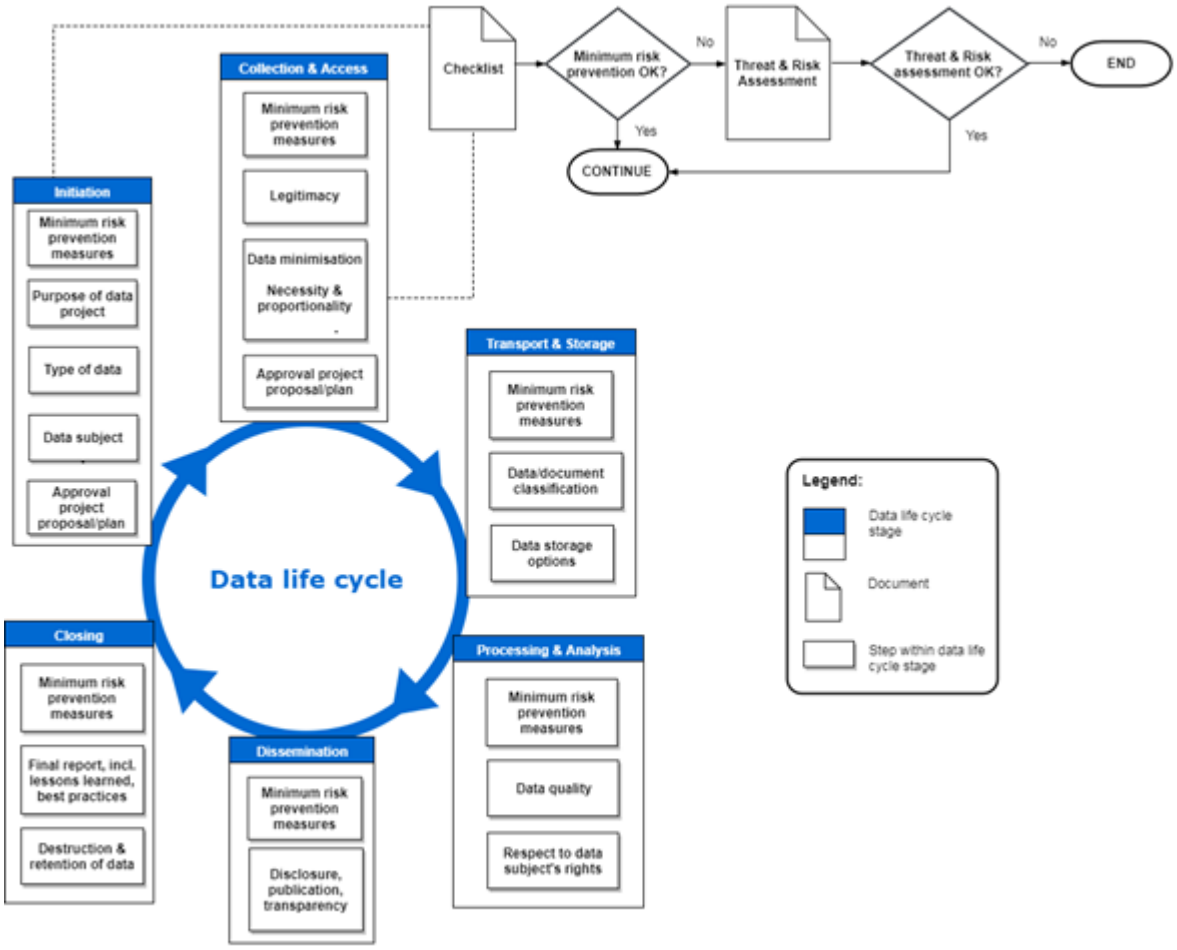
There are no specific requirements when handling anonymous data. It is recommended to conduct a risk and threat assessment at any time if there is a reason to believe data may be used to do harm to individuals or groups.

6. Data life cycle in different stages of project implementation

Figure 1 below illustrates how the principles and protocols interact during the life cycle of (data-driven) projects.

A data life cycle describes the stages that the data may undergo, from the moment the use of data is considered in a project until the data is destroyed. All stages are equally important and **they may occur in sequence or in parallel.**

Data life cycle in the different project stages



The data life cycle in a project, consisting of stages and steps. All stages are equally important and they may occur in sequence or in parallel.

The following table shows at which point in the data life cycle each team role is involved. For a more detailed description of the different team roles see annex.

	Data Team role							
Data life-cycle stage	*Data curator*	*Data owner*	*Data analyst*	*Data processor*	*Data controller*	*Data project lead*	*Data team lead*	*IT*
Initiation – anonymous data	■	■				■		
Initiation – Personal data, PII or DII	■	■			■	■	■	
Collection & Access – anonymous data	■	■	■					
Collection & Access – Personal data, PII or DII	■	■		■				
Transport & Storage – anonymous data	■							■
Transport & Storage – Personal data, PII or DII	■							■
Processing & Analysis – anonymous data			■					■
Processing & Analysis – Personal data, PII or DII				■	■	■		■
Dissemination – anonymous data	■					■		■
Dissemination – Personal data, PII or DII	■					■	■	■
Closing – anonymous data	■	■				■		■
Closing – Personal data, PII or DII	■	■				■	■	■

■ Specific data team role required

7. Implementation

The following minimum measures will be taken for practical enactment (i.e. implementation) of the policy.

a. **Welcome package and adherence to policy**

A first means of implementation will be to include reading the policy on data responsibility as an activity to the introduction package for new team members, as well as providing a printed copy of the policy to be signed for adherence in the course of their work.

b. **Training**

Bi-annual training sessions in responsible use of data will be held for team members. This component is essential in getting new team members up to speed on the responsible management of data, as well as refreshing the memories of existing team members. It is critical that the training in data responsibility is interactive and dialogical in nature.

c. **Communication and support**

A recurring task is to set up a means of reminding the team members about the importance of responsible data use. Additionally, it will refer members to the available resources (policy document, checklist, training resources etc.). Moreover, a dedicated communication channel aimed at answering questions about data responsibility will be put in place where all team members are invited and encouraged to ask questions and can receive guidance on how to apply the responsible use of data in the projects they are working on.

d. **Collection of lessons learned**

A collection of 'lessons learned' will be compiled to serve as examples of good and bad practices. Furthermore, the lessons learned collection will be a basis for educational purposes in data responsibility training and stimulating awareness.

ANNEXES/TOOLS:

Approval checklist [SHORT VERSION BASED ON THIS POLICY DOCUMENT]

The authority to approve on a project and its responsible use of data lies with [role in organization].

Dataset sensitivity classification

[INSERT METHODOLOGY USED]

It is recommended to use the IFRC Information Classification Standard (I.e. public, internal use only, restricted or highly restricted) and the definitions contained therein.

Document sensitivity classification

[INSERT METHODOLOGY USED]

It is recommended to use the IFRC Information Classification Standard (I.e. public, internal use only, restricted or highly restricted) and the definitions contained therein.

Third-party data sharing agreement template

[STANDARD TEXT TO BE DEVELOPED TOEGETHER WITH LEGAL]

Description of team roles

In this paragraph different team roles will be described in more detail, including any non-compatible roles.

Determine user permission policies associated with a dataset sensitivity classification.

[INSERT TOOL?]

Determine user permission policies associated with a document sensitivity classification.

[INSERT TOOL?]

Anonymization of PII or DII

METHODOLOGY TO BE DEVELOPED

Threat and risk assessment

i. A threat and risk assessment can be done for the project at any moment considered necessary. It is meant to identify the following questions: 'What threats does the data project pose for individuals or groups?' and 'What is the likelihood and potential impact?'
ii. Depending on the likelihood and consequences of the identified risks, additional mitigation strategies might need to be developed to execute the project or the decision might be made to abort the project. The way forward shall be decided in consultation with the team leads.

[INSERT TOOL]

IT requirements

Functional requirement	Preferred platform/solution
Internal communication	• MS Teams (Azure) • MS Planner (Azure)
External outlets	• Website (510.global) • Social media (Twitter/Facebook/LinkedIn)
External products	• Webviewer (based GeoNode server) • Kobo Toolbox & POSM server • CRA-dashboard (dashboard.510.global) • Github-pages
Internal data sharing	• Shared drive / network storage: MS Teams (Azure) • Shared PostGIS + Geo server (WFS/WMS): t.b.c. • Search mechanism / metadata
Internal product sharing (intermediate + final)	• Shared drive / network storage: MS Teams (Azure) • Storing QGIS projects also on network: t.b.d. • Search mechanism / metadata: t.b.d.
Server with computing power	• Network server with computing power: t.b.d.
Data protection	• Protocol & administrator for people to adhere to
Integration external sources	• Share data through services (webservices) • Links to HDX, OSM, IFRC, Worldbank

Figure 1: An initial set of functional requirements and preferred platforms/solutions.

Privacy by design

[GUIDANCE ON HOW TO APPLY PRIVACY BY DESIGN?] Covered by AZURE.

Standard disclaimer

The following disclaimer should accompany any map or dashboard data containing boundary data that is published:

> *"The maps used do not imply the expression of any opinion on the part of the Red Cross and Red Crescent Movement concerning the legal status of a territory or of its authorities".*