510 Data Responsibility Policy

Rationale behind this policy

For more than 150 years, the Red Cross has been guided by principles to provide impartial humanitarian help. The seven fundamental principles of humanity, impartiality, neutrality, independence, voluntary service, unity and universality were adopted formally in 1965. In the increasingly inter-connected world of the 21st century, upholding the validity of the fundamental principles has to go hand in hand with new technological developments and using new available resources to fulfill the mandate of helping the most vulnerable people around the world. In light of increased flows of information and (big) data, this means the Red Cross and Red Crescent Movement has an obligation to use the potential of these developments in providing humanitarian assistance. In times of vast humanitarian crises around the world and limited funding capacities, data can help to identify the most vulnerable people in need faster and prioritise more accurately the areas where help is needed the most. To this end, 510 is using data to improve the timeliness and (cost) effectiveness of humanitarian aid as well as preparedness and coping capacities for disasters and crises. Using data in a responsible manner is vital to ensure the applicability of the fundamental principles and to do no harm. The responsible use of data, a trend that is getting increasing recognition among major stakeholders, will shape the humanitarian ecosystem.[1] While legal instruments on data protection are an important step to enhanced transparency, data responsibility takes into account ethical considerations that go beyond compliance. Responsible use of data means bearing in mind the consequences the use of data could have on vulnerable people around the world and taking measures to avoid putting individuals or communities at risk. Acknowledging the important work that is already being done within the Red Cross and Red Crescent Movement[2] with regards to data protection in the humanitarian context, 510 hopes this policy will contribute to ongoing policy debates and exchange of experiences in this field, therefore encouraging the responsible use of data even beyond the 510 team.

Purpose of the policy

Given the context of 510's work on data-driven solutions for humanitarian aid, it is the purpose of this policy to incorporate principles for the responsible use of data in our daily work in a concise and workable manner. This policy will apply exclusively to the 510 initiative and is complementary to other applicable policies of the Netherlands Red Cross. New rules for the whole organisation, for example in light of the EU General Data Protection Regulation, will lead to further updates to this policy.

[1] Some of the key actors engaged in this topic are: UNOCHA, UNDG, UN Global Pulse, UNHCR, Danish Refugee Council, Oxfam, Harvard Humanitarian Initiative

[2] For one of the most recent and comprehensive publications, please see the 'Handbook on Data Protection in Humanitarian Action' published as part of a project by the Brussels Privacy Hub and the International Committee of the Red Cross (ICRC): https://shop.icrc.org/e-books/handbook-on-data-protection-in-humanitarian-action.html

Development of the policy

This policy has been drafted in a collaborative way by the Data Responsibility Project Team at 510. It is a result of extensive literature review, consultations with different departments of The Netherlands Red Cross and review by independent, external experts.[3]

The policy will be complemented by additional resources to ensure its implementation. This includes a *checklist* for a simplified use of the policy, guidelines for a *threat and risk assessment* in case the checklist raises 'red flags' (i.e. highlights potential risks) and *training materials*, including a collection of lessons learned.

Date of change of the policy Version 2.0: 8 November 2017

[3] We would like to thank the following experts for taking the time to review our 510 policy and providing valuable input: Prof. Dr. A.J. Zwitter from University of Groningen, Jos Berens from Leiden Centre for Innovation, Heather Leson from the International Federation of the Red Cross, Andrew Braye from the British Red Cross

1. Objective

The objective of this policy is to form the basis for how to handle data within the work context of the 510 initiative. It establishes principles that guide the responsible use of data and processes that help ensure their application. To complement the policy, specific implementation measures as well as material to raise awareness and train team members in their work will be developed. This policy is a 'living document', which will be updated over time if required by operational needs.[4]

2. Scope

This policy applies to all data used in the work of 510, whether within the team, in cooperation with other teams of The Netherlands Red Cross, or together with external third parties. All team members (staff, interns and volunteers) of 510 need to comply with the policy irrespective of the physical location where they carry out their tasks.

3. 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, assessments of the status and/or specific needs, 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)[5]

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

[4] Please consult the version date on the first page.
[5] Interchangeably, the common term Community Identifiable Information (CII) is used.

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

4. 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.

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 the fundamental principles of the Red Cross, especially with regards to putting humanitarian needs first while maintaining impartiality and neutrality.
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 510 initiative or by association the wider Red Cross/Crescent Movement.

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.

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. Exceptions may apply only if it is impossible to obtain consent (e.g. in an emergency) and the use of data is in the vital interest of the data subjects.

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

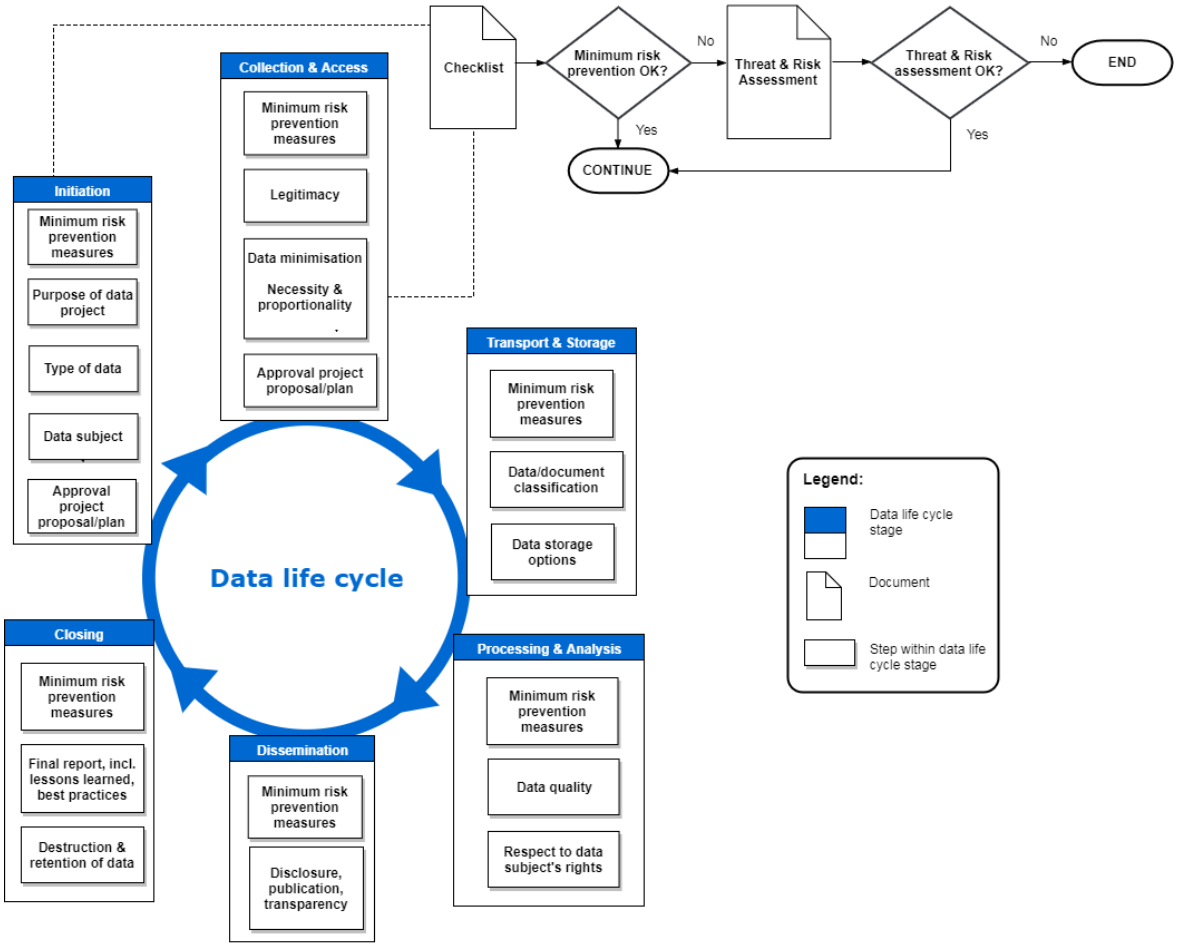
The data shall be as adequate, accurate, up to date, valid, reliable and relevant as possible for the specific purpose.

5. Data life cycle in the different project stages

Figure 1 below illustrates the life cycle of data(sets) visually adapted to common stages and steps within (data-driven) projects. These steps within the different stages are described in more detail as processes in section 6.

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.** Each stage consists of several steps that indicate an activity performed, or a property associated with the data. Some projects may not include all steps. Rather, the data life cycle is meant as a general guidance on the steps that need to be taken in most projects.

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.

6. Process steps in the different project stages

The processes outlined below incorporate the principles of the policy and serve to guide team members in the responsible use of data throughout different project stages.

6.1 Minimum risk prevention measures

The following risk prevention measures should be taken in every case and at every stage of the project:

a. **Follow this policy and use the checklist** to ensure application and look for potential risks i.e. 'red flags' (see 7.c.)
b. **Engage the local Red Cross/Crescent National Society** or other relevant local partner in the country of interest who is knowledgeable in the area of (data) policies and risks in the contextual setting of that country. This/these person(s) can then advise if and how to proceed. In this context, consider whether and how it would be possible to engage the local community.
c. **Ensure data security** (including IT security and special measures for sensitive data e.g. encryption, etc.)
d. **Apply the concept of 'privacy by design'** to each phase of the project from initiation to archival procedures. This means taking measures that increase privacy during the development of products or services and applying 'data minimisation' by collecting only data that is necessary for processing.

6.2 Initiation

a. Define Purpose

i. Define the purpose for which you will be using the data as narrowly, reasonably and practically as possible, and outline how it serves a humanitarian end.
ii. Data collection shall meet the purpose of the data project.

b. Type of data

i. Define the type of data you will be using over the course of your project.
ii. Examine whether you will be using Personal Data or Personally Identifiable Information.
iii. Examine whether you will be using Demographically Identifiable Information.

c. (Informed) consent from data subject

i. All reasonable efforts need to be undertaken to obtain informed consent from the data subjects to use personal data for the purpose of the project. Consent must be obtained at the time of collection or as soon as it is reasonably practical thereafter.
ii. The personal data cannot be re-used for other purposes than the consent was given for. Exceptions may apply only if it is impossible to obtain consent and the use is in the vital interest of the data subject.
iii. With regards to personal data, provide data subjects with an effective mechanism to request information on how their data is being handled, withdraw consent and have personal data corrected or deleted.

6.3 Collection & Access

a. Legitimacy and lawfulness

i. Always check if you have a legal basis for accessing and collecting the data. (see principle 4.e.)
ii. Before accessing data, always check for any licenses associated with it, which indicate the data ownership and the conditions under which the data may or may not be used.
iii. Check and comply with any terms, conditions and licenses of data providers. Note: copyright legislation differs from country to country.

b. Data minimisation

i. Apply 'data minimisation' and only collect data that is necessary for the pre-defined purpose of the project as well as proportionate and not excessive in scope.
ii. An initial time period needs to be set for the destruction of personal data in conjunction with the purpose of data collection and use. If the purpose of the data processing has not been completed by the end of the set time period, an assessment should be made on whether the data should be destroyed or if an extension of the time period of data retention is necessary. (see 6.7.a)

6.4 Transport & Storage

a. Classification of data/documents

i. Apply a dataset sensitivity classification[6] as part of the dataset's metadata.
ii. Apply a document sensitivity classification[7] on the first page or in the footer.
iii. Apply user permission policies associated with a dataset sensitivity classification.[8]
iv. Apply user permission policies associated with a document sensitivity classification.[9]

b. Storage options

i. Employ appropriate and reasonable technical and administrative safeguards (e.g. strong security procedures, de-identification of data) depending on the level of classification. (see 6.4.a.)
ii. Log the dataset with relevant metadata, including purpose specification (6.2.a), in an appropriate system.
iii. Before approaching Third parties for (online) services such as data storage, data retrieval or data processing, check if their policies are compatible with the principles of policy. Note that there may be significant differences in the terms and policies of the free and paid versions of the service.

6.5 Processing & Analysis

a. Quality

The following dimensions of quality shall be applied to ensure that (personal) data is adequately verified, validated and cleaned for further use and analysis:

[6] 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. Please contact the Team Leads to access this resource.
[7] Ibid.
[8] E.g. reading permissions, editing permissions, full control
[9] Ibid.

i. The relevance of the dataset shall be in line with the defined purpose of using the data (6.2.a).
ii. Evaluate the accuracy of the dataset e.g. in terms of completeness and any errors in the (personal) data, followed by correcting the errors in the (personal) data.
iii. Evaluate the timeliness of the dataset by checking when the data was released. Poor timeliness affects relevance (6.5.a.i) and accuracy (6.5.a.ii).
iv. The interpretability of the dataset shall be evaluated by checking for completeness and clarity (e.g. the use of full names for abbreviations in a dataset, clear headers in tables etc.) of the dataset.
v. If valuable in a given project, evaluate the comparability of the dataset by comparing the dataset with similar or related datasets in terms of coherence of data.

b. Respect to data subjects' rights

i. Respect for the data subjects' rights such as inclusion, dignity, informed consent, the right to verify their personal data, not to be put at risk, a right to privacy of their (personal) data and the protection thereof, shall be met. This means taking into account cultural and political contexts, as well as gender sensitive use of data.
ii. When processing and analysing data, one needs to bear in mind the consultations with local experts, data security and the concept of 'privacy by design' (see minimum risk prevention measures 6.1.b-c)
iii. When collecting, processing and using data, one needs to ensure that DII cannot be used to put groups and individuals at risk. (see 3.b. demographically identifiable information)
iv. It is advised to conduct a separate threat and risk assessment, if any doubts arise whether the data can be handled with respect to the data subjects' rights.

6.6 Dissemination

a. Disclosure, publication and transparency about project

i. Products produced by 510 (i.e. maps, online dashboards, infographics, other forms of information, etc.) shall not be shared publicly if they contain personal data/personally identifiable information of individuals or pose a significant[10] risk to groups of individuals. (see 4.c)
ii. Review the classification (6.4.a) and the storage options (6.4.b).
iii. Prior to publication, any communications about a project, or its products (e.g. via website or any other media channels) shall undergo a technical review of the publication, followed by evaluating the standard risk prevention measures (6.1).
iv. Any map or dashboards containing boundary data that are published shall be accompanied by a disclaimer mentioning "The maps used do not imply the expression of any opinion on the part of Red Cross and Red Crescent Movement concerning the legal status of a territory or of its authorities".

[10] A "significant" risk constitutes any identified risk higher than "low risk" (i.e. medium – critical risk). Please consult the Threat & Risk Assessment guidelines for further guidance.

6.7 Closing

a. Destruction and retention of data

i. Data should only be archived in situations in which doing so is based on a legitimate reason (e.g. for historical or scientific purposes, or for accountability of humanitarian action).
ii. Personal data and its metadata should be destroyed from all storage locations when the data is no longer necessary for the purposes for which it was collected, or when data subjects withdraw their consent for processing, or when data subjects object to the processing of their data.
iii. Inform the data subjects about a successful destruction of their personal data, in case of withdrawal of consent or objection to processing of their personal data.
iv. In case third party data storage products were used for storing personal data, obtain confirmation from the third party that the personal data was successfully removed.
v. Remove the personal data from the dataset and check the quality items (6.5.a).

b. Final report etc.

i. Final reports should also address the research methodology applied in the project, as well as the data sources and metadata used.
ii. Documentation such as signed contracts, copyright permissions, and final reports shall be archived centrally and retained as long as deemed necessary.
iii. An internal project evaluation shall take place between the project team and involved stakeholders to identify and share any best practices, bad practices and possibilities for continuous improvement.

6.8 Review and assessment of processes

a. Approval

The authority to approve on a project and its responsible use of data lies with the 510 team leads. However, each individual team member has the obligation to take action in complying with this policy.

i. Any project proposal/plan needs to be approved.
ii. If it is necessary to obtain an exception to use copyrighted materials for purposes other than those provided for (e.g. in the disclaimer), acquire written copyright permission from the content owner and attach it to the project proposal/plan.
iii. All approvals and permissions shall be archived.

b. Checklist

i. The checklist shall be used to follow the steps outlined in this policy and to evaluate if the requirements of minimum risk prevention measures are met.
ii. The checklist will highlight potential risks i.e. 'red flags' where there is no or only a partial compliance with the policy.

c. Threat and risk assessment guidelines

i. In case the checklist highlights potential risks i.e. 'red flags' for which the minimum risk prevention measures are not sufficient, a threat and risk assessment shall be done for the project. 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.

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 welcome package for new 510 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. Checklist

In line with this policy, a checklist is available in MS Word, which allows team members to easily apply the policy and to check for potential risks in a given project. The checklist creates a standardized output that controls whether what is being done complies with the policy.

d. Communication and support

A recurring task is to set up a means of reminding the team members about the importance of responsible data use.[11] 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.

e. 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.

[11] Specifically for 510: pop-up messages on Slack in the 510.global channel