

Data Responsibility Policy



Version 2.2 – Public use
12 November 2018

Keywords: data responsibility, data processing, policy

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.

Executive summary

Assessing the benefit of data-driven solutions in every humanitarian context versus their potential harm, requires awareness about how to use data technology and data in a responsible way. Humanitarian actors should take advantage of the opportunities provided by (open or closed) data, but they should do so responsibly.

When collecting and utilising personal data, the new EU General Data Protection Regulation imposes vital obligations upon organisations in terms of data protection. While conforming with data protection requirements is an important step to enhance transparency, data responsibility takes into account ethical considerations that go beyond compliance.

Data Responsibility accentuates the importance of data usage being lawful and legitimate. This means that access and use of the data have to be in accordance with applicable laws and agreements signed with third party data providers or recipients. Legitimacy refers to adhering to the organisation's own values and/or principles such as neutrality and impartiality in the case of the Red Cross/Red Crescent.

Responsible use of data means doing no harm and respecting each individual's fundamental right to privacy and to control the use and processing of his or her own personal data, bearing in mind the consequences that the use of data could have on vulnerable people around the world and taking measures to avoid putting individuals or communities at risk. The collection and processing of personal data may negatively impact vulnerable individuals or communities – despite the good intentions.

The use of data shall be guided by respect for the rights of the data subject, such as the fundamental right of protection of the personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage, but also dignity, informed consent, and not to be put at risk through the collection and use of data. Every individual who entrusts 510 with their personal data may request at any time to see a record of their data and to have these data altered or erased (right to be forgotten).

The collection and use of data for a specific dataset shall be guided by a pre-defined, practical and precise purpose for which the individual will be informed in advance. Personal 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.

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 need to be applied after a specific period, in accordance with protocols agreed upon in conjunction with the purpose of data processing.

The data shall be held against the highest quality standards to ensure minimisation, accurate and up to date representation of the data involved. 510 will ensure the same standards for third parties it will cooperate with.

Contents

| | |
|---|----|
| Executive summary..... | 2 |
| Reader's guide | 4 |
| Part I | 4 |
| 1. Introduction..... | 4 |
| 2. Purpose of the policy..... | 5 |
| 3. Principles | 6 |
| 4. Data life cycle: stages, steps and roles in a data project | 8 |
| Part II | 12 |
| 1. Initiation..... | 12 |
| 2. Collection and Access | 14 |
| 3. Transportation and Storage | 19 |
| 4. Data analysis | 27 |
| 5. Dissemination | 32 |
| 6. Closing | 33 |
| Annexes..... | 36 |
| A. Definitions | 36 |
| B. The rights of the data subject..... | 38 |
| C. Roles..... | 39 |
| D. Process..... | 42 |
| E. Registration form template for processing personal data | 47 |
| F. Methods anonymisation and pseudonymisation..... | 48 |
| G. Checklist template | 49 |
| H. Threat and risk assessment template | 49 |
| I. Third party data sharing agreement template | 49 |
| J. Standard disclaimer..... | 49 |
| K. Data collection tools | 50 |
| L. Data storage options | 54 |
| M. Basic metadata template | 55 |
| N. Preferred IT platform according to functional requirement..... | 56 |
| O. Creative Commons Licenses..... | 56 |
| P. Data breach procedure | 57 |

Reader's guide

This policy document is a practical guide for responsibly processing data in the projects and programmes carried out by the 510 data team and will be referred to as the “510 policy” throughout this document. The 510 policy is governed by the following sources developed by the Netherlands Red Cross (NLRC):

- “Privacy and Information security policy of the Netherlands Red Cross”, specifically for the aspects roles, responsibilities and tasks of members
- Appendix A of the “Privacy and Information security policy of the Netherlands Red Cross”: “*Privacy policy based on the General Data Protection Regulation (GDPR)*”, and
- Appendix B of the “Privacy and Information security policy of the Netherlands Red Cross”: “*Security measures*”

In order to keep the 510 policy concise, readers may be referred to specific sections of the above sources throughout the text for more details and background on the legal formulations and procedures. The 510 policy will be evaluated and updated over time based on the experiences of – and the feedback from – team members.

PART I

1. Introduction

Assessing the benefit of data-driven solutions in every humanitarian context versus their potential harm, requires awareness about how to use data technology and data in a responsible way. Humanitarian actors should take advantage of the opportunities provided by (open) data, but they should do so responsibly.

We define Data Responsibility as “the responsible processing of data with respect to ethical standards and principles in the humanitarian context, bearing in mind potential consequences and taking measures to avoid putting individuals or communities at risk”.

Data Responsibility encapsulates both data protection, the local and humanitarian context, as well as the ethical standards and principles as depicted in *Figure 1*.

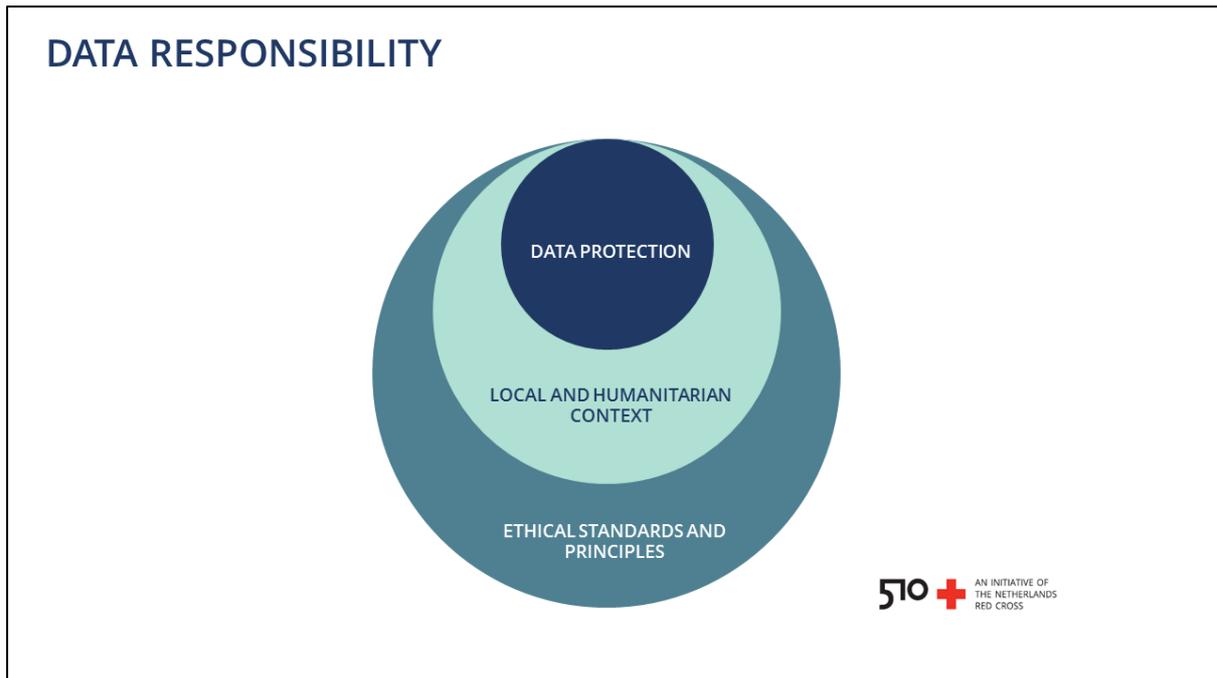


Figure 1 Data responsibility encapsulates both data protection, the local and humanitarian context, as well as the ethical standards and principles.

The importance of the responsible use of data is becoming increasingly recognised in the humanitarian field with key actors such as UNOCHA, UNHCR, Oxfam, Harvard Humanitarian Initiative, Brussels Privacy Hub and the International Committee of the Red Cross providing valuable insight and resources on the topic. Even so, acknowledging the important work that has already been done on the topic, 510 deemed it beneficial to provide a basis for how to handle data within the work context.

2. Purpose of the policy

Given that 510 is at its core a team dedicated to working on data-driven solutions for humanitarian aid, our policy has been designed for practical use. It ventures to incorporate the principles of Data Responsibility in our daily work for easy and functional application by our team members in various projects – the concise nature of the policy aids this goal. These principles are essential to our policy: each principle emphasizes vital considerations concerning the responsible use of data. For practical implementation the policy has been structured according to a data life cycle to provide general guidance on common stages and steps within (data-driven) projects.

The objective of this document is to ensure that all of 510's projects and programmes handle data in a responsible manner. This document consists of two parts. Part I provides the background and conceptual framework for the policy. Part II provides you with practical tools to prepare or update your project and to ensure it complies with this policy. It ends with a checklist that needs to be signed off by your manager before commencement of your project or after a review has taken place.

3. Principles

The policy is built upon the following principles of data responsibility¹:

1. Data protection



To protect data against unauthorized or unlawful access, use, accidental loss, damage or destruction, including during data transfers, reasonable administrative and technical security measures and privacy by design² processes shall be in place and observed.

2. Lawful and legitimate



Data shall be processed³ in such a way as to not infringe upon applicable laws or the legitimacy of the organisation.

Processing of personal data have to be in accordance with applicable law as well as the terms and conditions of third party data providers⁴.

All reasonable efforts need to be made to ensure that the core values and principles of the organisation are upheld. In the case of the Red Cross/Red Crescent Movement for example the principle of Humanity means to prevent and alleviate human suffering wherever it may be found; to protect life and health and to ensure respect for the human being.

3. Do no harm



All reasonable measures shall be taken to avoid causing any harm. This means considering the context of the project, including political and cultural sensitivities. For an accurate assessment local knowledge is essential and must be consulted. If at any time the use of any data or, conversely, not using data could pose significant risks to any concerned party, apply a qualitative threat & risk assessment. If the analysis reveals significant risks, one shall refrain from executing the project.

¹ These principles are derived from the GDPR, humanitarian principles and ethical standards.

² These are technical and organizational measures that take into account data privacy during the design stages of all projects along with the lifecycle of the relevant data process.

³ 'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. <https://gdpr-info.eu/art-4-gdpr/>

⁴ Consult a local lawyer or a legal specialist.

4. Respect for the rights of the data subject



The use of data shall be guided by respect for the rights of the data subject (see for more details appendix B: “*The rights of the data subject*”). Each data subject has:

1. the right to be informed about their personal data
2. the right to have access to their personal data and other specific information
3. the right to be informed about safeguards in case their personal data are transferred to a third country or to an international organisation
4. the rights of rectification and erasure
5. the right to restriction of processing
6. the right to data portability
7. the right to object at any time to (further) processing of personal data

All reasonable efforts shall be undertaken to obtain informed consent from the data subjects to use personal data for the purpose of the project. These data cannot be re-used for other purposes than the consent was given for. In the following cases⁵ data may be processed without prior written consent:

- a. processing is necessary for compliance with a legal obligation to which the controller is subject⁶;
- b. processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- c. processing is necessary for the performance of a task carried out in the public interest (example: Disaster relief);
- d. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party (example: Restoring Family Links)

Furthermore, data subjects are entitled to dignity and not to be put at risk through the processing of data. Everyone has a right to privacy, hereby not only considering their personal data but also Demographically Identifiable Information (DII) and the protection thereof.

5. Purpose specification



The processing of data for a specific dataset shall be guided by a pre-defined, practical and precise purpose. Personal 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.

⁵ Described in more detail in the “Privacy and Information security policy of the Netherlands Red Cross”.

⁶ For this and other reasons it is important to review applicable legislation and understand its implications during the design phase of the project.

Data subject's personal data will be destroyed after they have served the stated purpose. There are three exceptions to this: the data are needed to (a) exercise the right of freedom of expression, (b) there is a legal obligation to keep the data, (c) there are reasons of public interest such as historical value and for (academic) research, or (d) for defence in legal claims⁷.

6. **Minimisation (necessity and proportionality)**



The data we process shall be: (a) the minimum necessary to achieve the stated purpose, and (b) proportionate with regards to the envisioned humanitarian benefits and the potential for harm.

7. **Data quality**



The data shall be as minimal, accurate, up to date, valid, reliable and relevant as possible for the specific purpose to ensure the quality of the results of our analysis. The metadata assigned to the data may provide an additional characterisation of the data by considering aspects such as, but not limited to: confidentiality of the data, objectiveness of the data, comparability of the data in relation to other datasets, any participatory aspects of the data, etc. The metadata schema used shall be such that effective managing and searching of the data becomes possible, see annex M: "*Basic metadata template*".

4. Data life cycle: stages, steps and roles in a data project

A data life cycle describes the stages of processing that the data may undergo, from the moment the use of data is considered in a project until the data are destroyed, see *Figure 2*. All stages are equally important, but it may be that a project focuses only on one specific stage, or on several but not all stages. In case of several stages these may occur in sequence, or in parallel.

Stages have detailed activities known as steps, which in turn are linked to specific roles of team members. When designing a project you typically go through the stages Initiation, Collection & Access, and Transport & Storage first to prepare a project plan. Once your project plan has been approved, you "return" to Collection & Access to start the actual collection of data.

⁷ Described in more detail in the Privacy and Information security policy of the Netherlands Red Cross.

| Data processing stages | | | | | | |
|------------------------|--|--|--|--|--|--|
| | Initiation | Collection & Access | Transport & Storage | Data analysis | Dissemination | Closing |
| | Roles | Roles | Roles | Roles | Roles | Roles |
| | Team leads |
| | Project leads |
| | Information Manager | | Information Manager | | | |
| | Privacy Officer | | Privacy Officer | | | |
| | Security Officer | | Security Officer | | | |
| | Data controller | | | | | |
| | Data curator | Data curator | Data curator | | Data curator | Data curator |
| | Data owner | Data owner | | | | Data owner |
| | | Data analyst | | Data analyst | | |
| | | Data processor | | Data processor | | |
| | | | IT support | IT support | | IT support |
| Steps | Steps described in sub-section and annex |

Figure 2 The data life cycle, consisting of the data processing stages, the steps and associated roles.

A simplified organisational chart with representative **team roles** is shown in *Figure 3*. The chart shows the reserved leadership roles of Team leads, assigned leadership roles for Program managers and Project leads as well as the roles of project members within their

project teams. In addition to all these roles, the following **internal data specific roles** can be assigned:

- Data curator (exploring, updating and storing of data and metadata),
- Data owner (single-point-of-contact in a team for data ownership),
- Data controller (determines the purpose and means for processing data),
- Data analyst (exploring, processing, analysing and/or visualising data),
- Data processor (same as data analyst but processes personal data),
- IT support (maintains data storage solutions, data protection software, etc).

In small project teams, each team member may need to fulfil more than one internal data specific role.

- Team leads can take on the roles of Program managers or Project leads (if need be). Only they can be Data controllers. They are **overall accountable** for data responsibility compliance.
- Program managers and Project leads are **responsible** for data responsibility compliance in their teams.
- The internal data specific roles “Data controller” and “Data processor” differ in roles and responsibilities as compared to the “Data controller” and “Data processor” roles mentioned in the GDPR. GDPR Data processors for example are always third party, non-NLRC organisations/companies who process data on our instruction and solely on written agreement.

There may be also **specific organisational roles** for staff providing e.g. legal expertise and advice (“Privacy Officer”, PO), security expertise and advice (“Security Officer”, SO), or information management expertise and advice (“Information Manager”, IM). All these roles are also shown on the organisational chart. The team roles, internal data specific roles and the specific organisational roles are collectively referred to as “roles” in this document. The definitions of the roles can be found in annex C: “Roles”. In *Part II* these roles will be specifically linked to the data life cycle steps.

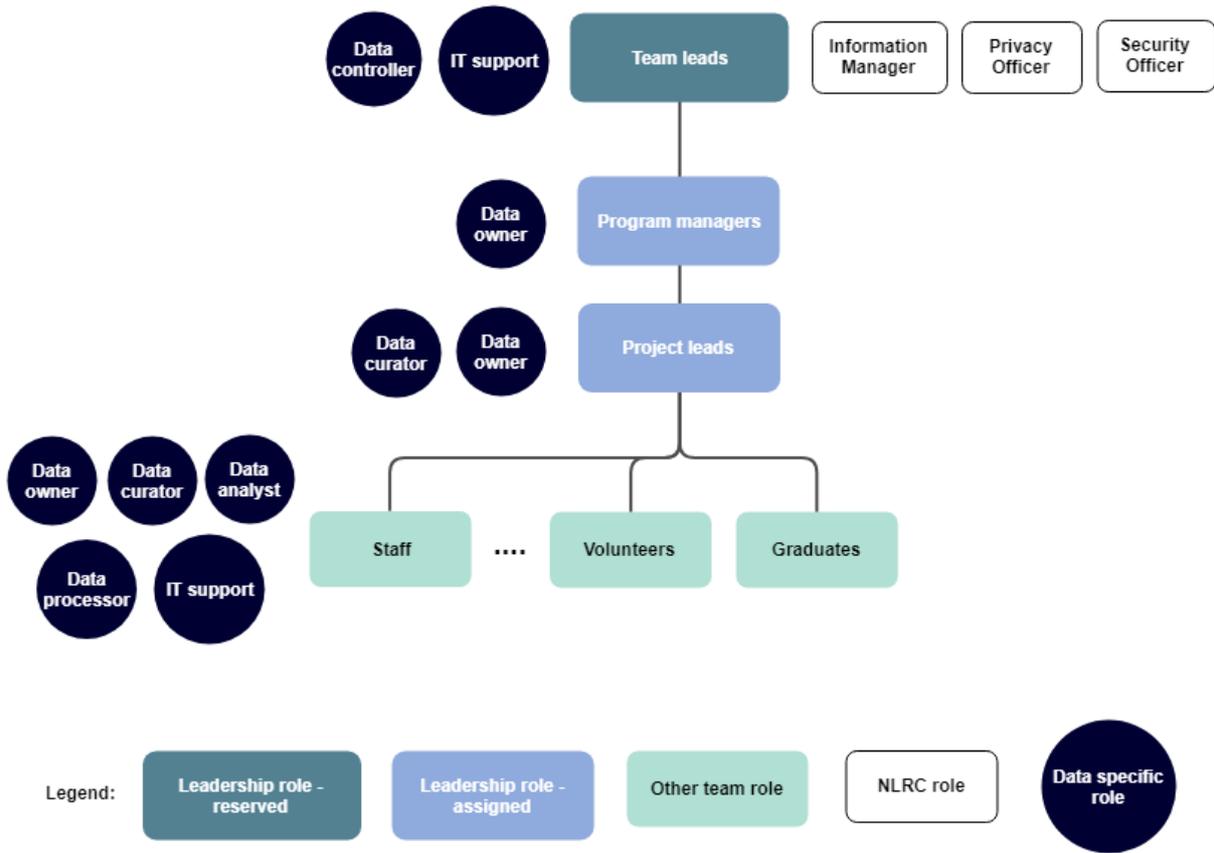


Figure 3 An organisational diagram showing the team roles and the internal data specific roles at 510. The roles indicated by Information Manager, Privacy Officer and Security Officer are organisational specific roles at the Netherlands Red Cross (NLRC). The definitions, responsibilities and tasks are mentioned in annex C.

PART II

Part II of this policy document describes which role(s) is/are involved in each of the stages of the data life cycle. Some practical tools and methods are described at the end of each section to help you prepare or execute your data project in a data responsible way.

1. Initiation

A high-level overview of the Initiation stage, steps and roles is shown in *Figure 4*. This stage marks the starting point for the design phase of the project when preparing a project plan. See annex "*Stage Initiation*" for the roles and steps in more detail.

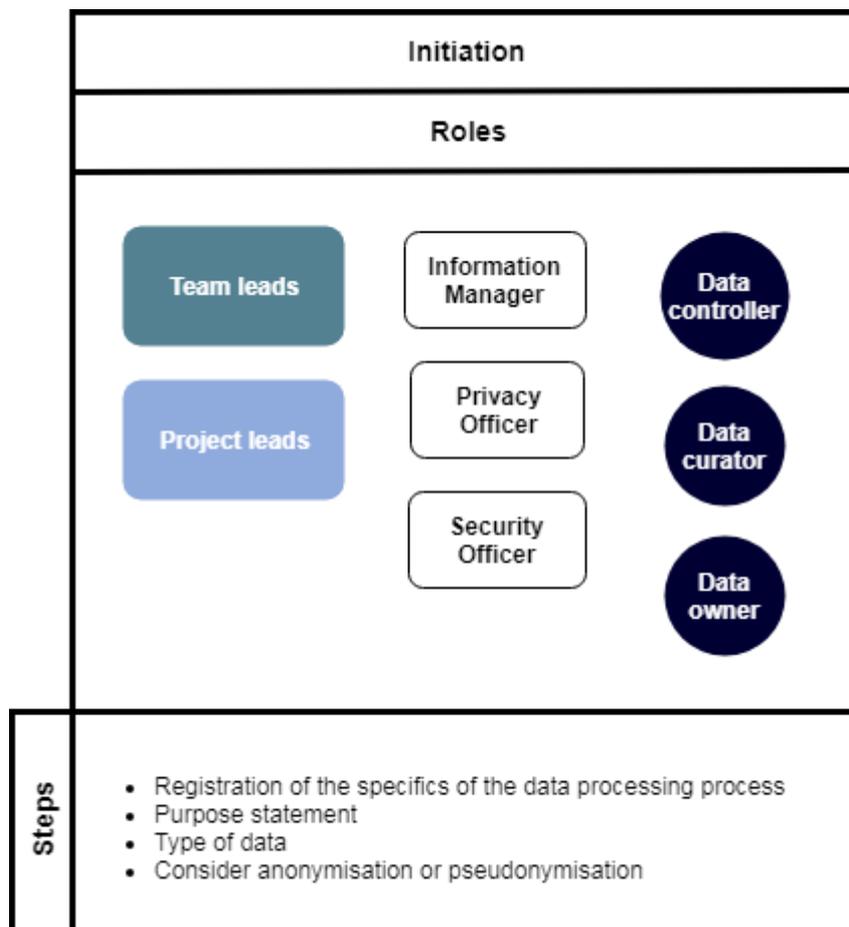


Figure 4 Initiation stage with roles and steps.

1. Registration of the specifics of the data processing process

If personal data are going to be processed, a registration form needs to be filled in by the Program manager/Project lead, capturing essential information about the processing activities, see annex E: "*Registration form template for processing personal data*". The registration form captures for example:

- The purpose of processing

- The lawful and legitimate reason(s) for processing
- The categories of data subjects, e.g. staff, donors
- The categories of persons (according to their job titles) who have access to the data
- The retention period after which the various categories of personal data need to be deleted, or any considerations for determining the retention period

The registration form needs to be reviewed and signed-off by the PO or SO at the end of the design phase, before continuing with the next stage of the data life cycle. The approved registration form is then documented and registered by the IM.

2. Purpose statement

The foundation for the project is laid when formulating the purpose statement. This statement will influence every aspect of the project and shall be specific, concise and time bound in nature. You should also indicate the time when you intend to erase all personal data collected.

3. Type of data

The second step is to determine what type of data will need to be processed as part of specific deliverables of your project. This policy distinguishes the following types of data:

- Personal Data:

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 multiple individuals, e.g. 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. Personal Data or DII can be anonymised and become anonymous information, provided the raw/unprocessed information has been deleted from all storage locations, mobile data collection phones, and shredded in the case of paper documents.

4. Anonymisation and pseudonymisation

The third step is to consider anonymising, pseudonymising or encrypting datasets. When working with multiple types of data, there may be a need to combine or relate them. It is important to keep in mind that when **unrelated datasets are combined or related**, even if each dataset only contains anonymous data, the resulting dataset may enable the identification of individuals. This is also known as the ‘mosaic effect’.

Depending on the purpose and risk involved for using anonymous data and/or Personal Data and/or DII, specific methods can be considered for anonymising, pseudonymising or encrypting the combined dataset during the “Data analysis” stage (see annex E: “*Methods anonymisation and pseudonymisation*” for an overview of these methods and several examples).

Note:

1. If personal data in datasets have been **anonymised** for processing, the datasets are no longer considered to be of the type personal data.
2. Even if your current source dataset, having anonymous data, may not enable the identification of individuals, this may still become possible later because of new datasets becoming available and the ‘mosaic effect’.
3. If personal data in datasets have been **pseudonymised** for processing using keys, the datasets are still considered to be of the type personal data, if the keys and original datasets have not been deleted from all storage locations, mobile data collection phones, and shredded in the case of paper documents.
4. Essential for pseudonymisation is that the key holding the translation to the originally entered data should always be stored at a (virtually) remote place that cannot be accessed from, or at the same time, as the pseudonymised data.

2. Collection and Access

A high-level overview of the Collection and Access stage, steps and roles is shown in *Figure 5*. See annex “*Stage Collection & Access*” for the roles and steps in more detail. This stage is also part of the design phase of the project when preparing a project plan. The Project lead is ultimately accountable for his/her project towards the Team lead and responsible for ensuring everyone involved understands their respective roles. Updating the checklist and the risk log help the Project lead keep control over each stage.

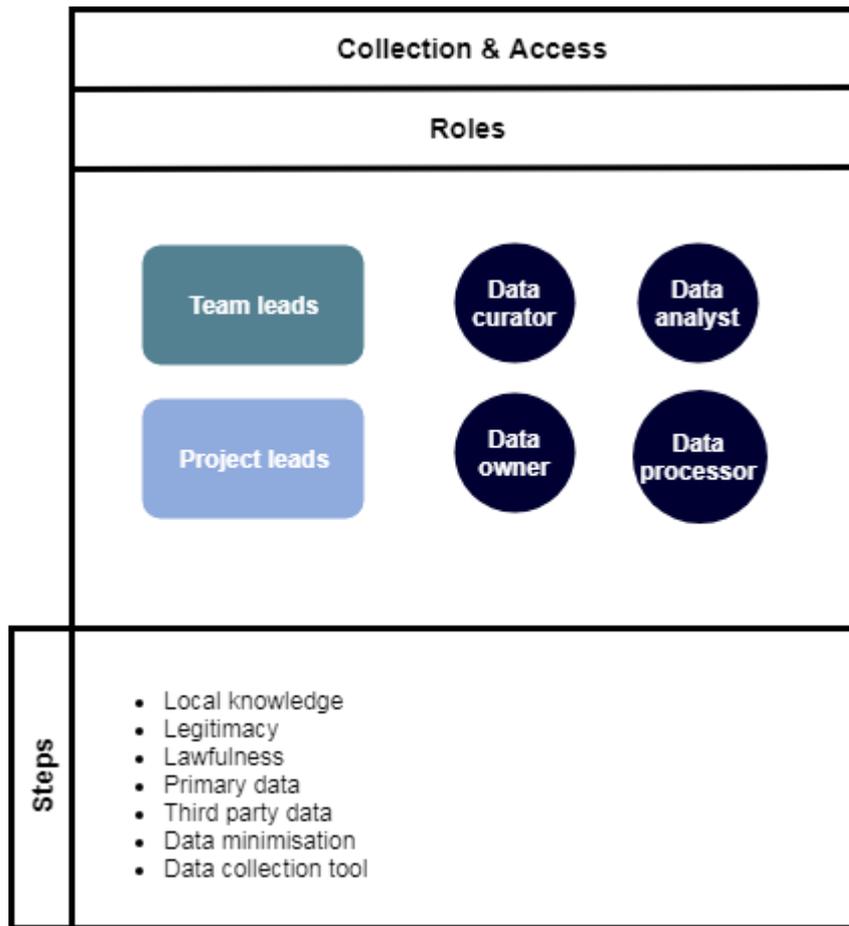


Figure 5 Collection & Access stage with roles and steps.

1. Local knowledge

Local knowledge is very important and can prevent problems from occurring as your project moves forward. Make sure to 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.

2. Legitimacy

Revisit your organisation’s core values and principles and ensure that you are working within them.

3. Lawfulness

Check the applicable legal framework of the country to ensure that you have a valid **legal** basis for collecting and/or accessing the data. As we are a Dutch organisation we always need to take the GDPR in account, wherever we operate.

You must also have a valid **lawful**⁸ basis in order to process personal data. Most lawful bases require that processing is ‘necessary’. If you can reasonably achieve the same purpose without the processing, you won’t have a lawful basis. You can lawfully process personal data based on, amongst others, the following arguments:

- **Consent:** Consent means offering individuals real choice and control through a positive opt-in. Do not use pre-ticked boxes or any other method of default consent. It should always be possible for 510 to provide proof of the actual given consent per individual.
- **Legitimate interest:** Legitimate interests means the processing of personal data without consent is essential for the primary, essential activities/processes of the NLRC⁹:
 - i.e. in case of emergency/disaster relief
 - in the context of fundraising activities

Only applicable if not entailing or risking the breach of fundamental rights of the data subjects. Disclosing personal data to a third party may rely on legitimate interests in case of actual emergency relief operations.

- **Vital interest:** Vital interests are intended to cover only interests that are essential for immediate life/death situations. If there are less intrusive ways, e.g. if the individual is capable of giving consent, this basis will not apply. You are likely to be able to rely on vital interests as your lawful basis if you need to process the personal data to protect someone’s life. Processing of one individual’s personal data to protect the vital interests of others is likely to happen more rarely. It may be relevant, for example, if it is necessary to process a parent’s personal data to protect the vital interests of a child.

4. Primary data - collecting data from data subjects directly

Obtain informed consent from the data subject(s) to process their personal data for the purpose of the project. Consent requires a positive opt-in. Do not use pre-ticked boxes or any other method of default consent. Keep evidence of consent – who, when, how, and what you told people (i.e. the consent statement used). 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 items¹⁰:

⁸ As described in the GDPR.

⁹ Described in more detail in the “Privacy and Information security policy of the Netherlands Red Cross”.

¹⁰ For detailed description of individual rights, see “Principle 4: Respect for the rights of the data subjects” and Annex A.

- i. The purpose of the data collection.
- ii. Describe how data subjects can verify their personal data, request information on how their data is being handled, withdraw consent and how they can have personal data corrected or erased.
- iii. The guarantee that the personal data they provide is not re-used for other purposes than the consent was given for.
- iv. Name any third party controllers who will rely on the consent.
- v. Destruction of their personal data after the project closes and/or after a specified retention time **unless** the data are needed to (a) exercise the right of freedom of expression, (b) there is a legal obligation to keep the data, (c) there are reasons of public interest¹¹, or for defence in legal claims¹².

5. Third party datasets

When using third party datasets¹³, verify if any additional rules or restrictions apply to your data source(s):

- a. Check the original consent of the data subjects and the information they have received on the purposes for the collection and processing of their data. This information should include explicit consent for use by explicitly designated third parties. If informed consent is not available, check on the possibilities for processing without consent.
- b. Check any terms, conditions and licenses of third party data providers. Note: copyright legislation differs from country to country.
- c. 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.
- d. Check if you need to acquire a written copyright permission from the content owner.
- e. 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).
- f. Record any licenses or permissions with the datasets they pertain to.

¹¹ These exceptions are mentioned, amongst others, in the General Data Protection Regulation: <https://gdpr-info.eu/art-17-gdpr/>

¹² ¹² Described in more detail in the “Privacy and Information security policy of the Netherlands Red Cross”.

¹³ Third party data are sometimes referred to as “secondary data”.

- g. Should the third party from whom you are obtaining data not offer an agreement, please use the third party data sharing agreement template in the annex of this policy document.

6. Data used for creating and enriching digital maps in OpenStreetMap

Maps are an important source of information in preparing before and managing an operation after a disaster. For large areas detailed maps are not available or have a quality which does not suit the needs at that time.

To obtain better quality data and so to make better decisions, there are several options. One of these options is Missing Maps.

Missing Maps is a project to map these areas with large numbers of (mainly non-experienced) volunteers by interpreting satellite images and drawing the objects (buildings, roads, etc.) on a digital map (OpenStreetMap). The participation of many volunteers results in a higher capacity to map areas quickly and so to quickly have more data available. These data will be available at OpenStreetMap as Open data and can therefore be shared with anyone for further use. However, a copy of these data can be used to enrich the data with more project related data. Afterwards it can be decided, based on confidentiality of the data if these data can be shared openly or not.

7. Data minimisation



Data minimisation as a standard practice throughout your project makes sense not only from a cost control perspective; the less data you process the less risk you run of causing harm with these data.

Data minimisation implies that you only process data that are necessary for the pre-defined purpose of the project, that are proportionate and not excessive in scope.

8. Data collection tools/methods

The following is a non-exhaustive list of data collection tools commonly used:

- Before collecting data, check what data are already available.
- Before selecting and applying an Open Mobile Data collection tool such as Kobo Toolbox, Mega V, Magpi, POSM, etc, evaluate their functional properties. See annex K: "*Data collection tools*" for a detailed description.

- Before collecting open data from public websites and portals using methods such as automated or manual web scraping, manual downloading, Application Programming Interfaces (APIs), etc. evaluate the criteria and conditions associated with processing of those datasets. At 510, several scripts are available upon request for automated web scraping.
- Before using satellite imagery or drones to capture areal images in a particular (area of a) country, ensure looking at the lawfulness of using such technology in that particular country.
- In the case of personal data that are initially collected on paper and are subsequently digitized (such as surveys), ensure responsible handling of these data for both the interviewees/respondents and the interviewers/enumerators conducting the survey. The same holds in case an interview is initially digitally recorded (by means of a video camera, a web camera or a voice recorder) and is then transcribed for reporting purposes at a later stage.

3. Transportation and Storage

This stage is the final part of the design phase of the project in which the project plan is finalized. Once your registration form for the processing of personal data has been approved by the Privacy Officer or Security Officer and subsequently documented and registered by the Information Manager, and the Team lead has approved the checklist, threat and risk assessment and project plan, you return to “Collection and Access” to start the actual collection of data.

A high-level overview of the Transportation and Storage stage, steps and roles is shown in *Figure 6*. See annex “*Stage Transportation & Storage*” for the roles and steps in more detail.

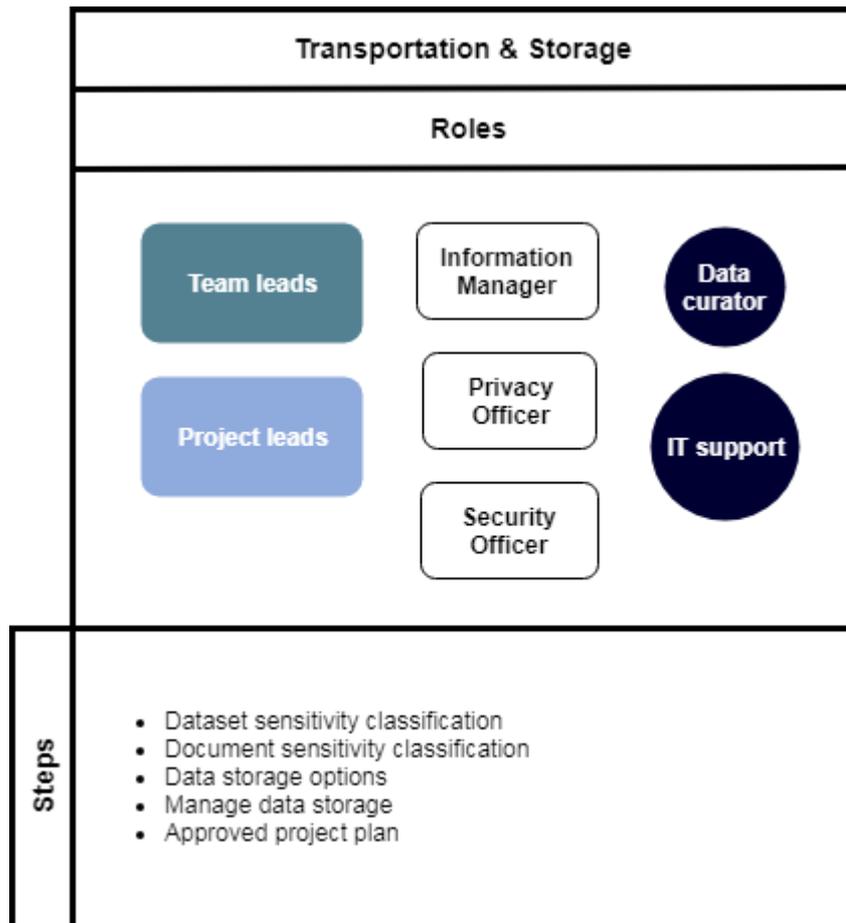


Figure 6 Transportation & Storage stage with roles and steps.

1. Dataset sensitivity classification

It is recommended to use an Information Classification Standard (i.e. public, internal use only, restricted or highly restricted) and the definitions contained therein, as applied by your organisation.

As a rule of thumb any dataset containing personal data should be classified as “highly restricted”.

2. Document sensitivity classification

It is recommended to also use an Information Classification Standard (i.e. public, internal use only, restricted or highly restricted) and the definitions contained therein for documents.

As a rule of thumb any document containing personal data should be classified as “highly restricted”.

3. Data storage options

For an overview of data storage options see annex L: “Data storage options”. When setting up your data storage system it is important to take into consideration the rights of the data subject, especially their right to be forgotten and the right to have their data updated.

When working with datasets or documents that contain personal data, i.e. have been classified as “highly restricted”, you shall apply data minimisation here as well by centralising the storage of data to one suitable data repository system¹⁴, thereby preventing duplicates of datasets or documents to be stored across multiple data repository systems. When storing personal data outside of NLRC servers, processing agreements need to be concluded with these parties. You can consider using one of the following storage options at 510 (see *Table 1 and Table 2*), but only after consulting the Security Officer (SO):

Table 1 The storage options at 510 and the classification level categories for the availability, integrity and confidentiality of these systems when storing personal data. The number values have been omitted in this public version of the 510 policy.

| Storage option | Data type(s) | Ownership & maintenance storage | Classification level | | |
|---------------------------------|---|---------------------------------|----------------------|-----------|-----------------|
| | | | Availability | Integrity | Confidentiality |
| Shared-drive in MS Azure | <ul style="list-style-type: none"> Personal data Anonymous data Pseudonymous data DII | NLRC | | | |
| MS Teams | <ul style="list-style-type: none"> Anonymous data Pseudonymous data Personal data | 510 | | | |
| Magpi | <ul style="list-style-type: none"> Anonymous data Pseudonymous data Personal data | 3 rd party: Magpi | | | |
| GeoNode | <ul style="list-style-type: none"> Anonymous data Personal data DII | 510 | | | |
| HDX | <ul style="list-style-type: none"> Anonymous data | 3 rd party: HDX | | | |
| Google drive | <ul style="list-style-type: none"> Anonymous data Pseudonymous data | 3 rd party: Google | | | |

¹⁴ Generally it is the safest choice to store personal data in as few locations as possible. Situations involving digital identities such as those used in blockchain applications may diverge from this logic and offer safe storage of sensitive data on multiple personal devices rather than one centralised location.

| Storage option | Data type(s) | Ownership & maintenance storage | Classification level | | |
|------------------------------------|--|---------------------------------|----------------------|-----------|-----------------|
| | | | Availability | Integrity | Confidentiality |
| Dropbox | <ul style="list-style-type: none"> • Anonymous data • Pseudonymous data | 3 rd party: Dropbox | | | |
| External hard disk | <ul style="list-style-type: none"> • Personal data • Anonymous data • Pseudonymous data | 510 | | | |
| USB sticks and memory cards | <ul style="list-style-type: none"> • Anonymous data | 510 | | | |
| Laptop | <ul style="list-style-type: none"> • Varies | NLRC | | | |
| UAVs | <ul style="list-style-type: none"> • Anonymous data • Personal data • DII | 510 | | | |

Table 2 An overview of the storage options used by 510, and several of their properties and functionalities.

| Storage option | Pros | Cons |
|---|--|---|
| Shared-drive in MS Azure | <ul style="list-style-type: none"> Secured network drive Access permissions on individual level Storage capacity can be easily increased as needed | <ul style="list-style-type: none"> Requires set-up by helpdesk at Netherlands Red Cross No metadata options |
| MS Teams | <ul style="list-style-type: none"> Password management Regular backups Software upgrades | <ul style="list-style-type: none"> No role-based access permissions such as read-only, editing, full-control etc. No metadata options |
| Magpi <ul style="list-style-type: none"> End-user mobile device Central server | <ul style="list-style-type: none"> Data protection measures: password management, device encryption, secure connection | <ul style="list-style-type: none"> None |
| GeoNode (GIS content) | <ul style="list-style-type: none"> In-house data storage with full control over access permissions Ability to share through services (control over data quality) Metadata capabilities | <ul style="list-style-type: none"> No control over who uses/shares the data, so if data are open they can be used by the entire world. |
| HDX (Humanitarian Data eXchange) | <ul style="list-style-type: none"> Storage of public and private datasets Basic set of metadata options required Searching of datasets | <ul style="list-style-type: none"> Requires indication of license type for sharing content |
| Google Drive (mobile app and desktop app) | <ul style="list-style-type: none"> Data protection measures: password management and 2-step verification Role based access permissions: read-only, editing | <ul style="list-style-type: none"> Each file type (Google Docs, Google Sheets etc) has its own max file size Not to be used for storage of personal data No metadata options |
| Dropbox (mobile app and desktop app) | <ul style="list-style-type: none"> Data protection measures: password management Encryption of files during transport to server and when at rest at server location Role based access permissions: owner, editor, or viewer | <ul style="list-style-type: none"> Free account allows up to 2 GB of disk storage space Not to be used for storage of personal data No metadata options |

| Storage option | Pros | Cons |
|--|--|---|
| External hard disk (not advised unless suitable data protection measures are taken) | <ul style="list-style-type: none"> • Easy backup of large volumes of data | <ul style="list-style-type: none"> • Data not automatically encrypted • Use of cable-lock needed to make it theft-proof |
| USB-stick/memory cards (not advised unless suitable data protection measures are taken) | <ul style="list-style-type: none"> • Easy backup of small volumes of data on a small device | <ul style="list-style-type: none"> • Data not automatically encrypted |
| Laptop | <ul style="list-style-type: none"> • Data protection measures: password management, device encryption, virus scanning | <ul style="list-style-type: none"> • Use of cable-lock needed to make it theft-proof |
| Unmanned Aerial Vehicles (UAVs) | <ul style="list-style-type: none"> • For low data volumes: local onboard data storage • For high data volumes: upload to cloud storage service using a wireless connection | <ul style="list-style-type: none"> • Local onboard data storage needs to withstand crashes from high altitudes, be waterproof in case of water incidents and be resistant to elevated temperatures • Requires data encryption • Wireless connection to cloud service needs to be secure • Spoofing: UAVs are susceptible to hijacking by unauthorized persons taking over the wireless control of UAVs • UAVs are not theft-proof (e.g. after a crash) |

4. Managing your data storage option

After deciding what data storage option you are going to use, please ensure that you record the following as an integral part of your dataset, and that you apply appropriate technical and administrative safeguards.

Record consent statement

1. Record the consent statement used with each dataset for future reference. Check, if any of the four legitimate reasons for processing the personal data without consent applies (see Principle 4: “Respect for the rights of the data subject”)

Maintain a list of all storage locations

2. Create and maintain a list of all storage locations where personal data relevant to the project are stored, including storage locations of third parties in case data are shared.

Time period for destruction

3. Set the time period for the destruction of personal data in conjunction with the purpose of data collection and use. This includes confirming with third party recipients, that they have erased the data from all their storage systems. Any personal data that is anonymised can be kept if there are no other serious concerns that come out of a threat and risk analysis.
4. Enable finding and destroying single data records without affecting the quality of the overall data set.

Apply/review user permission policies

5. Apply “privacy by design” principles to each phase of the project from initiation to archival procedures.
6. Apply user permission policies associated with a dataset sensitivity classification (e.g. reading permissions, editing permissions, full control).
7. Apply user permission policies associated with a document sensitivity classification (e.g. reading permissions, editing permissions, full control).
8. When team members move to other roles within the team and/or leave the team, review their access policies.

Apply technical and administrative safeguards

9. Employ appropriate and reasonable technical and administrative safeguards (e.g. strong security procedures, de-identification of data) depending on the level of classification.
10. In principle do NOT store datasets with Personal Data or DII in cloud-based platforms based on collaboration functionalities such as Google drive. Anonymise or pseudonymise your dataset before uploading it to such platforms.
11. Latest SQL servers may have built-in scripting options to automatically anonymise or pseudonymise database entries. In case encryption/decryption keys are used, these shall be stored separately from the dataset. The keys shall be accessible only for authorized members.
12. When transferring your data to a remote database/server, always use a secured connection. Secure transfers can be done over encrypted tunnels, Virtual Private Networks (VPN's) and/or using secure file transfer protocol applications (S-FTP).
13. When storing data on external devices such as hard disks, usb sticks, portable servers etc use data encryption with password protection.
14. Hard disks of laptops can also be encrypted, using methods such as: 1. 'full disk encryption', protecting your device when it is powered off, but not when it is powered on, or 2. 'two-layer encryption of folders', where one password is used to only reveal several folders, whereas a second password needs to be used to reveal all other hidden folders. In case encryption may be a reason for concern when crossing international borders, consider entering with an empty storage device. If possible, check the country's policy for encrypting devices.
15. Apply good password management ethics:
 - a. Regularly change passwords for each of your sites, tools, databases, laptops, smart phones, etc. ensuring that each of these resources has a unique password.
 - b. Assign one person in a project team for updating passwords and providing access to resources.
 - c. When providing a password, use a single strong master password and all other passwords are randomly generated using 20+ characters.
 - d. Apply two-factor authentication, e.g. "LastPass", "GlobalSign", "Google Authenticator", etc.

- e. Especially on smart phones use numerical screen-locking instead of pattern based screen-locking; your fingerprints on the screen may reveal your pattern for unlocking your phone.
- f. All MS Office applications have settings to make them “password protected”. However, these password protection schemes are weak and so can be (easily) cracked by several of the commercially available password recovery programs.

5. Approve project plan

At this point you should finalise your project plan and first obtain approval for the Registration form from the Privacy Officer (PO) and/or Security Officer (SO) and then register the completed form with the Information Manager (IM). The Security Officer and the Privacy Officer only need to be consulted if your project proposes a new, not yet reviewed way of processing data.

- Role of IM in case of a “new, not yet approved way of processing data”:

The IM is consulted. Together with the process owner the IM decides whether or not (a) the processing of data can be considered a new process, or (b) that it appears to be new but is comparable to what has already been registered, or (c) that it does not appear to be new but considering items indeed has to be considered as being new and if in this case a single modification would allow the processing to become part of an already existing overarching registration, or (d) if a new registration still has to be performed.

- Role of IM in case of “not new, or not yet approved way of processing data”:

The IM will always cross-check the processing of data with existing registrations to check if there is an addition/deviation, for example if data are transferred to other/new/additional parties, other data processors, etc.

Following the approval of the IM you should obtain approval from your Team lead. After this you can start the implementation of your project and the actual collection of data.

4. Data analysis

A high-level overview of the Data analysis stage, steps and roles is shown in *Figure 7*. See annex “*Stage Data analysis*” for the roles and steps in more detail.

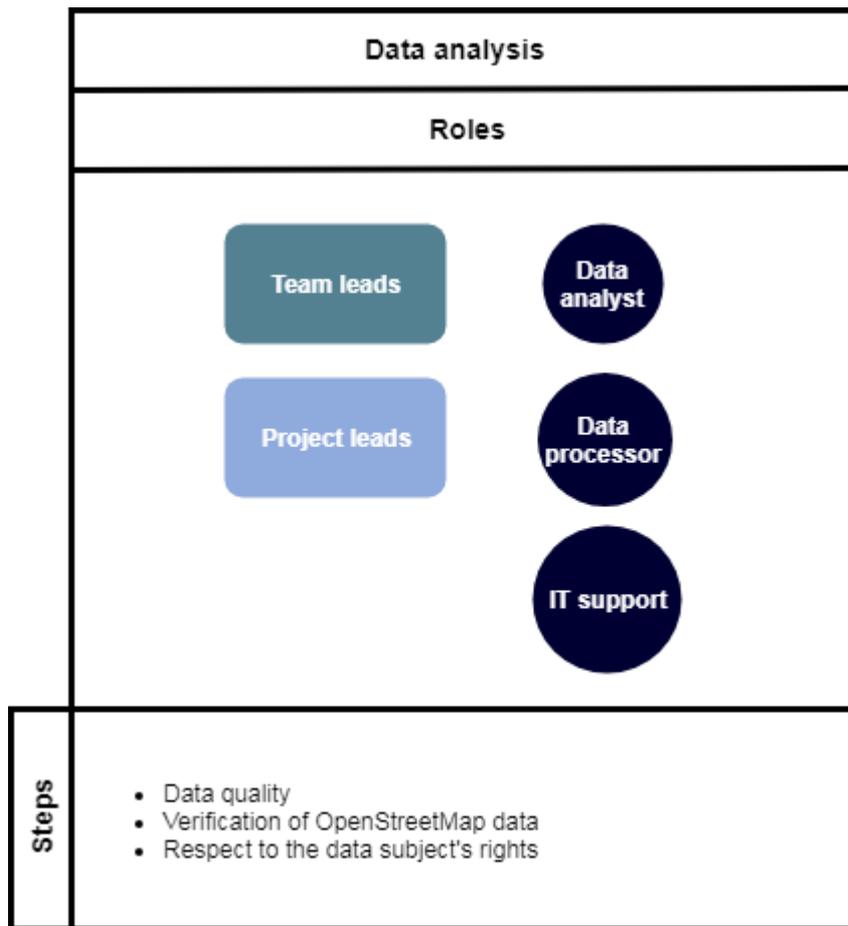


Figure 7 Data analysis stage with roles and steps.

Processing of the (raw) dataset during the Data analysis stage consists of two main steps, related to data quality and respect for the rights of the data subject. An intermediate step exists in case OpenStreetMap data need to be verified.

1. Data quality

- Data quality assessment, which focuses on inspecting and evaluating the properties of the (raw) dataset and its metadata in terms of minimisation, completeness, relevance, timeliness, etc
- Anonymising, pseudonymising or encrypting the personal data in the (raw) dataset
- Data quality enhancement, based on the inspection and evaluation of the data quality properties followed by cleaning the dataset

- Applying (statistical) analyses methodologies to derive insights from the dataset in relation to the purpose of the project. The type of methodology and tools are left to the judgement of the Data processor/Data analyst
- Generate/update metadata for the analysed dataset by using a “metadata standard” with a schema that is suitable for a specific data storage option (see annex M: “*Basic metadata template*”). A summary of the types of metadata, their purpose, the abbreviation code of the metadata standard and an example of a data storage option using that metadata standard, is shown in *Table 3*.

2. Verification of OpenStreetMap data

In Chapter 2 Collection & Access, it was described how Missing Maps data can add value during data collection. The following steps can be used to verify the data.

The Missing Maps coordinator divides an area into small tiles for each volunteer to map. After the initial mapping, another person checks the mapping activities.

Checking consists of three steps:

Step 1: visual check of each tile

- are all the required objects mapped?
- do these objects have the right tag?
- is the outline of the object in accordance with the satellite image?

Step 2: checks on logical rules

For example: two buildings on top of each other, a road nearly connecting to another road, a road crossing a building. For this purpose, a special program has been developed (JOSM), which checks a tile in terms of many of these types of rules.

Step 3: overall check

Differences between tiles: e.g. a road ends on the edge of a tile, a road changes its classification (tag) on the edge, a river changes the direction of the stream at the edge of a tile or becomes a canal.

In general, everybody can do the validation. It is possible to restrict the validation to “approved” validators, but there are no instruments or criteria for appointing someone as a “validator”.

After validating, field checking improves the mapping: adding names on the map, adding functions of buildings, adding small elements (e.g. water taps), improving road

classification (e.g. a mapped road proves to be not suitable for cars and is therefore changed into a path).

3. Respect to the data subject's rights



- Your privacy notice should include your lawful basis for processing as well as the purpose of the processing. If your purpose changes, you may be able to continue processing under the original lawful basis if your new purpose is compatible with your initial purpose. You may also be able to continue processing if you can argue legitimate interest or another lawful basis. Documentation of the arguments is essential as part of the Registration form.

Table 3 An overview of the types of metadata (i.e. information about information), and the storage systems applying those metadata types.

| Type of metadata | Purpose | Metadata standard | Data storage option |
|--------------------------------|--|---|--|
| Descriptive metadata | All metadata that can help users to: <ul style="list-style-type: none"> Identify information resources Locate information resources Retrieve information resources | <ul style="list-style-type: none"> ISO 19115: 2003(E) – Geographic Information CSW (Catalogue Service for Web) HDX standard (user must indicate a minimum set of metadata entries). See also Humanitarian eXchange Language: http://hxlstandard.org/ | <ul style="list-style-type: none"> GeoNode HDX |
| Technical metadata | Metadata that contain information about technology e.g. <ul style="list-style-type: none"> database ownership physical characteristics of database | <ul style="list-style-type: none"> T.b.d. | <ul style="list-style-type: none"> T.b.d. |
| Administrative metadata | Metadata to help manage administrative aspects of a database e.g. <ul style="list-style-type: none"> intellectual property rights licenses for data usage | <ul style="list-style-type: none"> HDX standard (user must indicate a minimum set of metadata entries) | <ul style="list-style-type: none"> HDX |
| Use metadata | All metadata used by administrators to: <ul style="list-style-type: none"> Manage user access Manage user tracking to e.g. monitor how often authorised and non-authorised users logged-in, accessed a document, or modified it Manage multi-versioning information | <ul style="list-style-type: none"> HDX standard (user must indicate a minimum set of metadata entries) | <ul style="list-style-type: none"> HDX |
| Preservation metadata | All metadata used for documenting actions to preserve data, e.g. <ul style="list-style-type: none"> Migrations of data Checksum calculations to check integrity of data | <ul style="list-style-type: none"> T.b.d. | <ul style="list-style-type: none"> T.b.d. |

5. Dissemination

A high-level overview of the Dissemination stage, steps and roles is shown in *Figure 8*. See annex "*Stage Dissemination*" for the roles and steps in more detail.

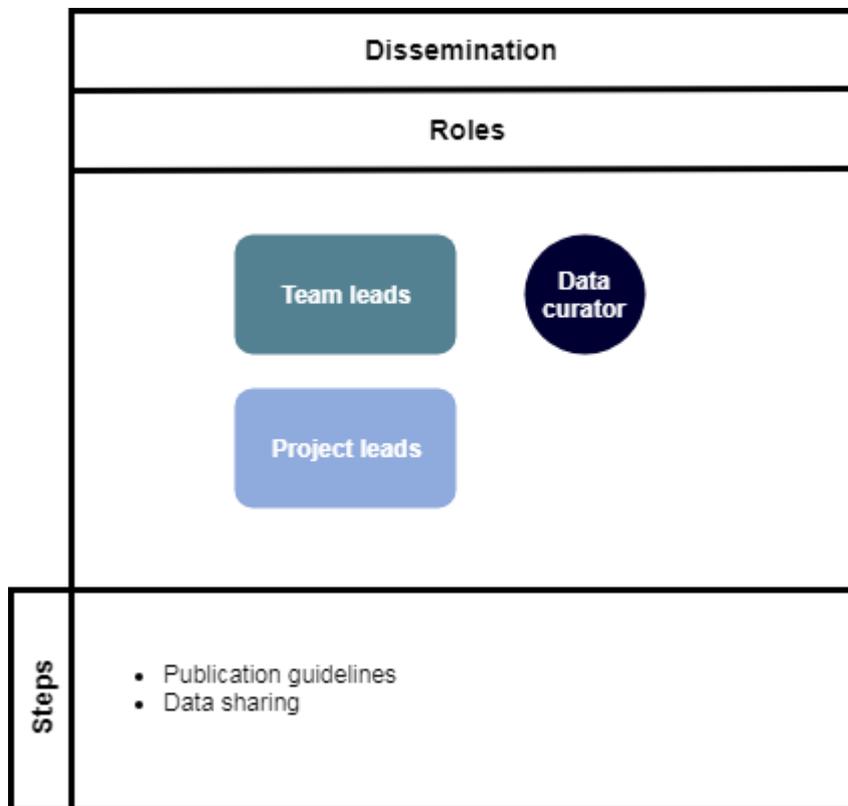


Figure 8 Dissemination stage with roles and steps.

Publication guidelines

- a. No personal data or products containing personal data shall be shared or disseminated publicly. Only anonymised or pseudonymised products (products from which all personal data have been deleted) may be disseminated publicly.
- b. Prior to the dissemination (e.g. via a website or any other media channels) of any communications or information products, a threat and risk assessment must be conducted (see annex H: "*Threat and risk assessment*"). In case any threat is identified, a sensitivity classification has to be given to the document or product and the Team lead needs to sign off on the communications product.
- c. 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". A standard disclaimer can also be found in annex J: "*Standard disclaimer*".

- d. After publication, data shared through online platforms should come with a proper data sharing license. See annex O: "*Creative Commons Licenses*" for some guidance on selecting a Creative Commons license, as well as this [online tool](#). A general disclaimer should always accompany publication on correctness of the data and changes after date of collecting the data. All datasets need to be dated. The data sharing platform should restrict indexing and caching of datasets.

Data sharing

Should you be requested access to a dataset, you must ensure that you:

1. Have the authority (typically the data curator) to grant access to this dataset
2. Provide access within the limitations set forth in the consent statement and or any applicable third party data sharing agreement¹⁵.
3. Use the data sharing agreement template provided in the annex of this policy document.

Please refer to annex I: "*Third party data sharing agreement template*". This template should be used when providing data to third parties and can be used when receiving data from third parties.

6. Closing

A high-level overview of the Closing stage, steps and roles is shown in *Figure 9*. See annex "*Stage Closing*" for the roles and steps in more detail.

¹⁵ The only exceptions to this limitation is when the data are 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. Consult a local lawyer to verify how these exceptions must be documented.

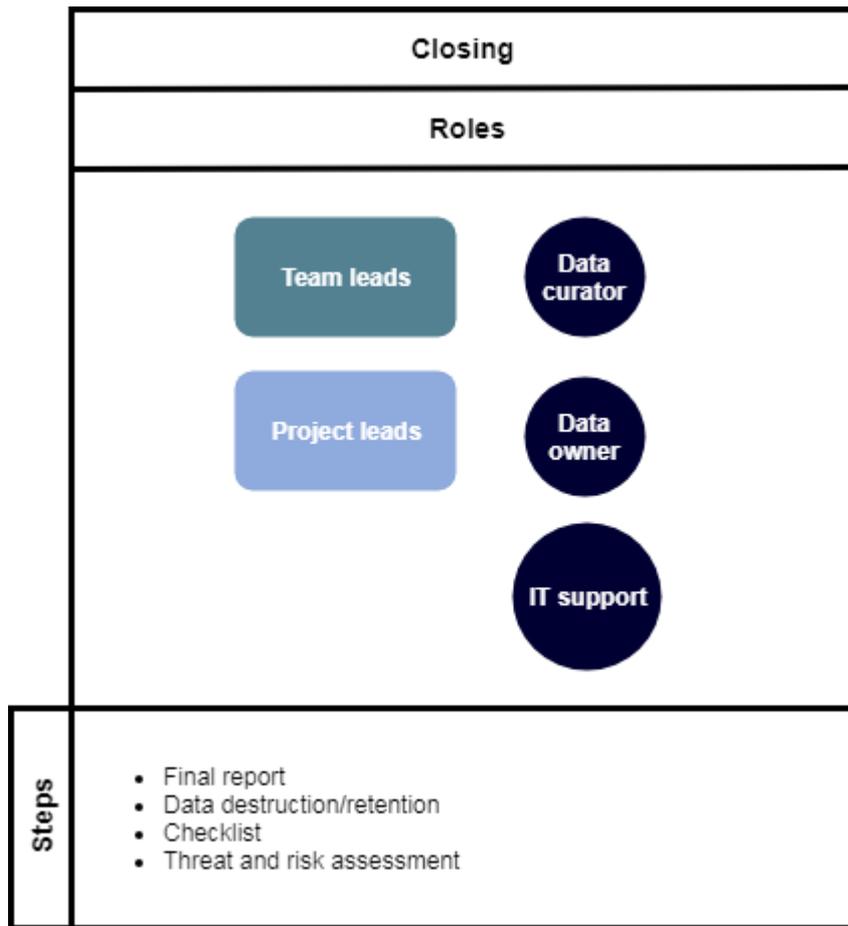


Figure 9 Closing stage with roles and steps.

Final report

In consultation with your Team lead determine whether an evaluation on data management practices during the project would be useful. In particular when data related incidences or data breaches occurred (see the procedure in annex P: “Data breach procedure”) for a final evaluation, looking in depth at these issues is required. Otherwise cover data responsibility in your general project evaluation exercise. Ensure that your final reports address the research methodology applied in the project, as well as the data sources and metadata used.

Data destruction/retention

- a. Obtain confirmation from all third party storage providers that any personal data were successfully removed after closure of the project.
- b. Ensure that any personal data and their metadata are destroyed from all storage locations. Paper-based documents containing personal data, such as surveys, need to be shredded.

- c. Any data that will be retained must be anonymised.
- d. Only personal data that meet exception criteria¹⁶ and are properly documented may be retained in a secure location.
- e. Centrally archive and retain documentation such as signed contracts, copyright permissions, and final reports as long as deemed necessary.
- f. Archive all permissions and approvals.
- g. Delete consent forms, if no longer needed.

Publication guidelines

When disseminating the final project results, refer to the publication guidelines as described under the “Dissemination” stage (see previous section).

¹⁶ Documented cases only concerning data that are needed to (a) exercise the right of freedom of expression, (b) there is a legal obligation to keep the data, (c) there are reasons of public interest, or (d) for defence in legal claims.

Annexes

A. Definitions

For this policy the following terms and definitions are applicable:

a. Personal Data & Personally Identifiable Information (PII)

‘Personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person¹⁷.

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.

The term Personal Data in the context of the GDPR covers a much wider range of information, such as social media posts, lifestyle preferences, transaction histories etc. Therefore, in this policy the term Personal Data will be used.

b. Demographically Identifiable Information (DII)¹⁸

¹⁷ Definition as used in the GDPR.

¹⁸ Interchangeably, the common term Community Identifiable Information (CII) is used.

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. The Data Subjects' consent/clear affirmative action may be given either by a written statement or an oral, audio recorded statement. One should note that agreeing to a disclaimer or using data under a license can be a clear affirmative action.

The Data Subject needs to be informed on the processing of its data prior to giving its consent. The necessary information can be included in a privacy statement for which the Data Subject must have had the opportunity to read or otherwise to be explicitly informed on.

e. 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, partners we work with, within or outside of the Movement, agencies providing online services for storing personal data, etc.

B. The rights of the data subject

1. The right to be informed about:
 - a. the identity and the contact details of the controller
 - b. the contact details of the data protection officer
 - c. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing
 - d. If the data were not acquired on the basis of informed consent: the legitimate interests pursued by the controller or by a third party
 - e. the recipients or categories of recipients of the personal data, if any (meaning third party recipients)
 - f. where applicable, the fact that the controller intends to transfer personal data to a third country or international organization;
 - g. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
 - h. the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability
 - i. the existence of the right to withdraw consent at any time,
 - j. the right to lodge a complaint with a supervisory authority
 - k. whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
 - l. the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

When the data have been acquired from a third party, additionally:

- m. the categories of personal data concerned
 - n. from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;
2. Right of access to the personal data and the following information, which will need to be provided within reasonable time from the request and in an appropriate matter:
 - a. the purposes of the processing;
 - b. the categories of personal data concerned;
 - c. the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
 - d. where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
 - e. the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

- f. the right to lodge a complaint with a supervisory authority;
 - g. where the personal data are not collected from the data subject, any available information as to their source;
 - h. the existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
3. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer
 4. Rights of rectification and erasure
 5. Right to restriction of processing
 6. Right to data portability
 7. Right to object at any time to (further) processing of personal data

C. Roles

The internal data specific roles at 510¹⁹

Data curator: A team member tasked with exploring, updating and storing of (open) datasets, metadata information and other relevant document properties in a well-structured central database or repository system, ensuring that the datasets and documents are easily searchable and accessible for analyses. This role is sometimes referred to as “data steward” or “data manager”. This is not a role/responsibility as per the GDPR.

Data owner: Single-point-of-contacts in a team (i.e. Project manager, Project leads, volunteers, etc) tasked with keeping track of any legal documents such as proof of consent of Data subjects, 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 owners may indicate the access policies of the data sets and documents, as per the legal agreement/contract, to the Data curator. In case Data subjects wish to see their personal data, or have their personal data removed, or processed differently, the Data owner communicates this to the data Project lead, Data curator and Data processor.

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

¹⁹ See also: “Privacy and Information security policy of the Netherlands Red Cross”, section roles, responsibilities and tasks of members

Data processor: Identical to the role of Data analyst, except the data are now of the type Personal Data or DII. Data processor as an internal role differs from the Data processor role mentioned in the GDPR. According to the GDPR, Data processors are always third party, non-NLRC organisations/companies who process data on our instruction and solely on written agreement.

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

Program manager: A team member tasked with managing several (related) projects, each of them led by Project leads.

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.

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, assigning/withdrawing access permissions, first point of contact for team members in 510 to report a security breach and overall accountable for data responsibility compliance at team level.

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

The NLRC roles related to Privacy & Information Security (P&IS)

Please refer to NLRC's latest "information security policy, and the privacy policy attachment A" for more details on the roles and responsibilities of the Security Officer (SO), Policy Officer (PO) and Information Manager (IM).

Security Officer (ICT, technical): The Security Officer (SO) is responsible for preparing and executing the policy for information security. The responsibility entails:

1. Serving as a security advisor for management in case of drastic changes in the ICT-infrastructure, monitoring the realisation and development of automated processing in case of changes in systems and applications,
2. Coordinating the execution of measures for information security according to the information security policy/plan and supporting projects in which information security plays an important role,

3. Supervising the registration of information security incidents in the information security registers,
4. Advising Information Managers about the settlement of incidents and evaluation of the incidents in conjunction with the Privacy Officer (PO).

Privacy Officer (Legal): The Privacy Officer (PO) is responsible for:

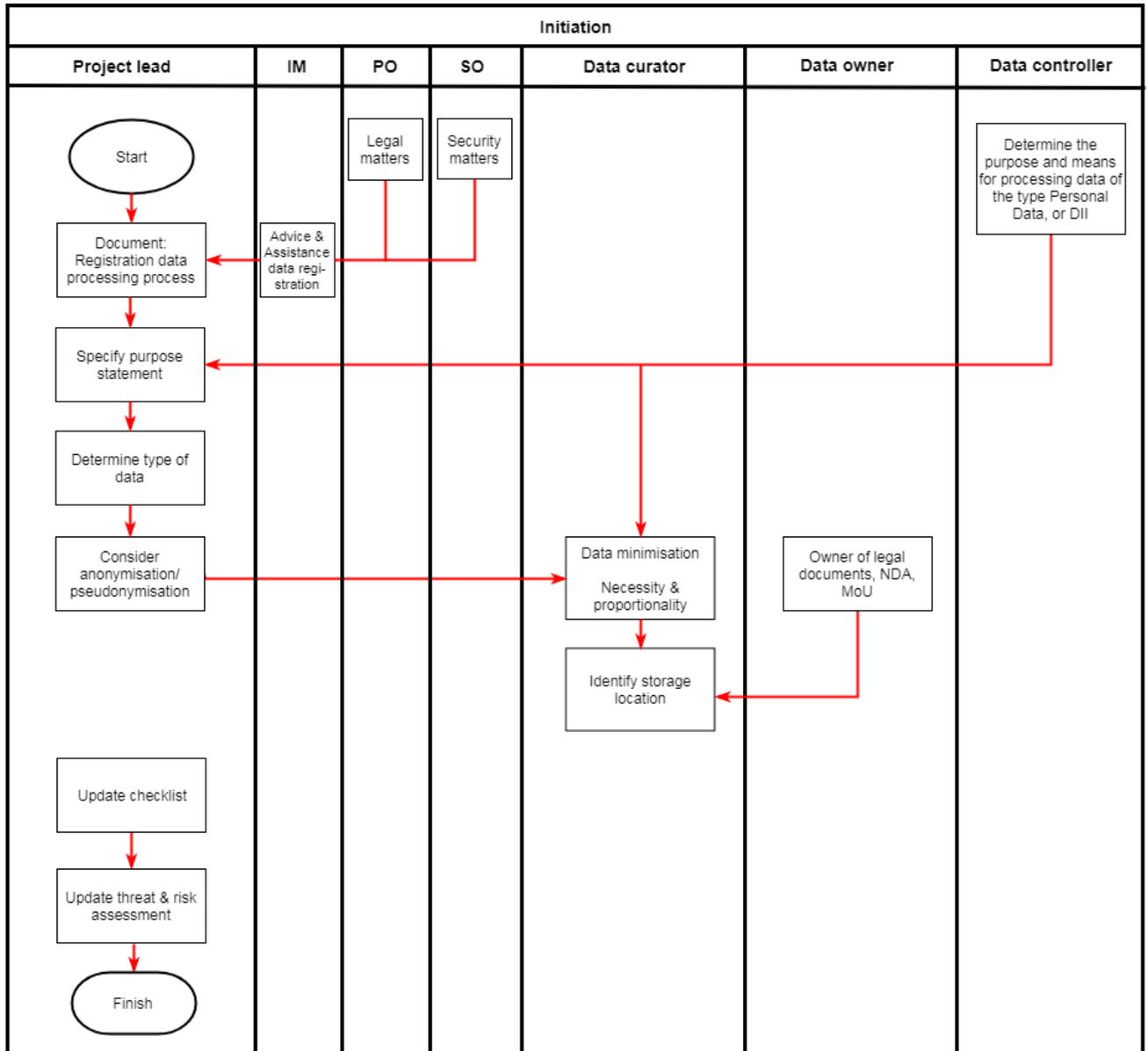
1. Informing users of systems in relation to processing of personal data and informing of Information Managers in relation to the registration and processing of personal data,
2. Providing legal advice on the execution of rights of Data subjects involved, informing of Data subjects involved, privacy statement on a website, reporting of security breaches, contracting of new Data processors and establishing of data processing agreements,
3. Upon request, providing advice or assistance in the execution of a Privacy Impact Assessment (PIA) and any resulting improvements thereof,
4. Serving as a single-point-of-contact on behalf of the NLRC for the Dutch “Data Protection Authority” (DPA).

Information Manager (functional support, end-user support): The Information Manager (IM) has a:

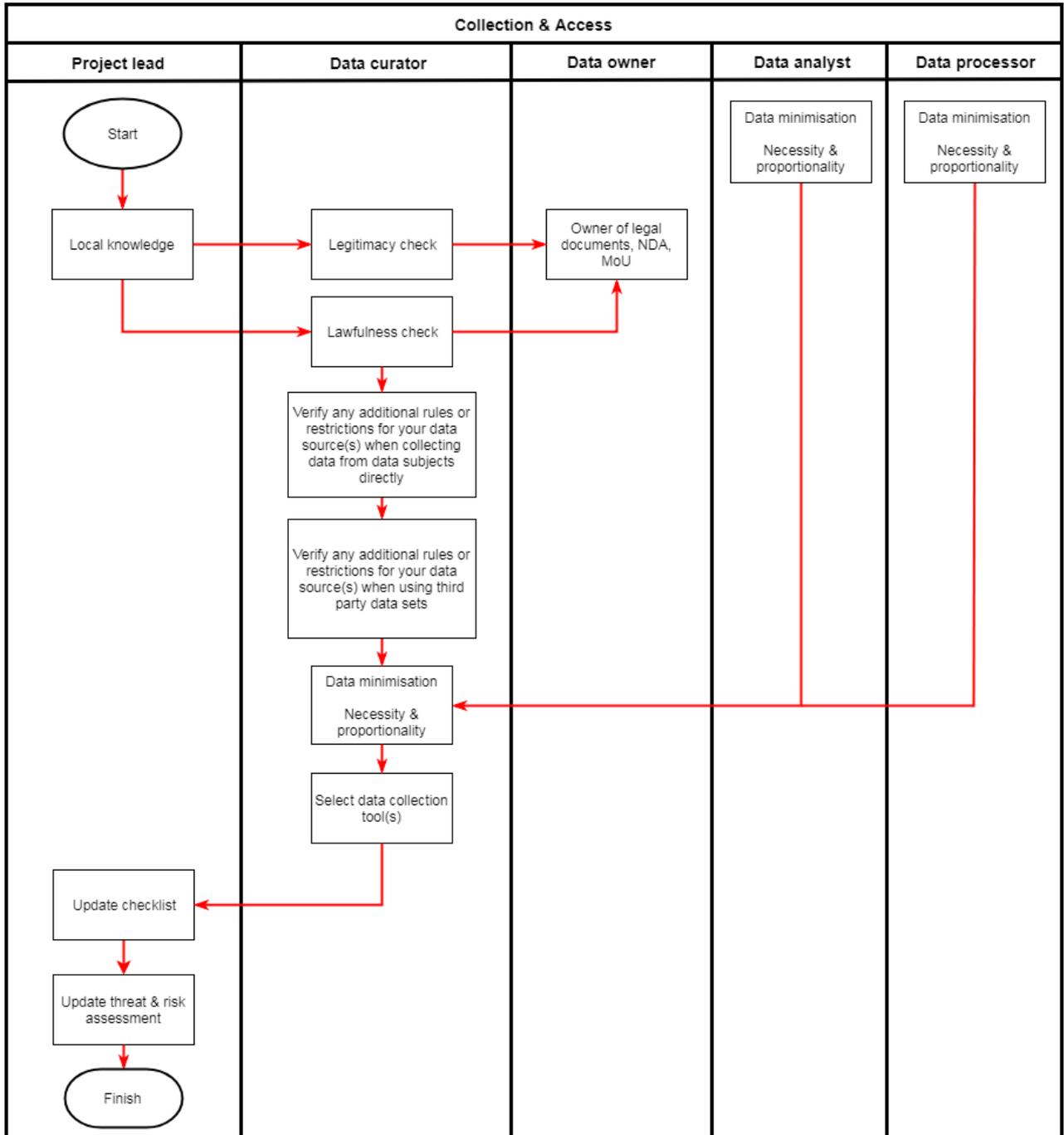
1. Coordinating role regarding the registration of the processing of personal data,
2. Role in registering and settling data incidents and security breaches, for which IMs advise and support follow-up,
3. Responsibility in optimally aligning the applications being used with the needs of the cluster.

D. Process

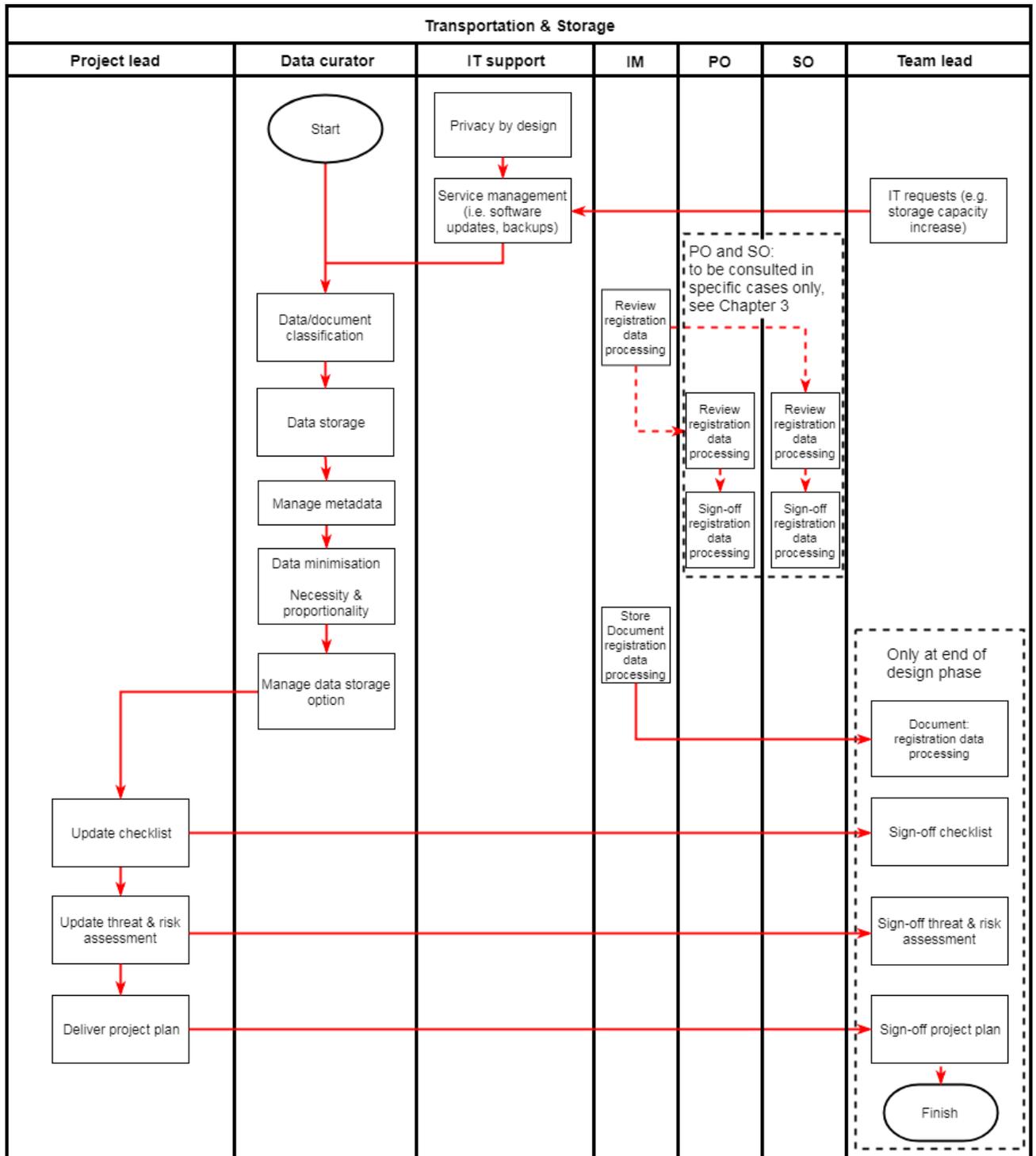
Stage Initiation



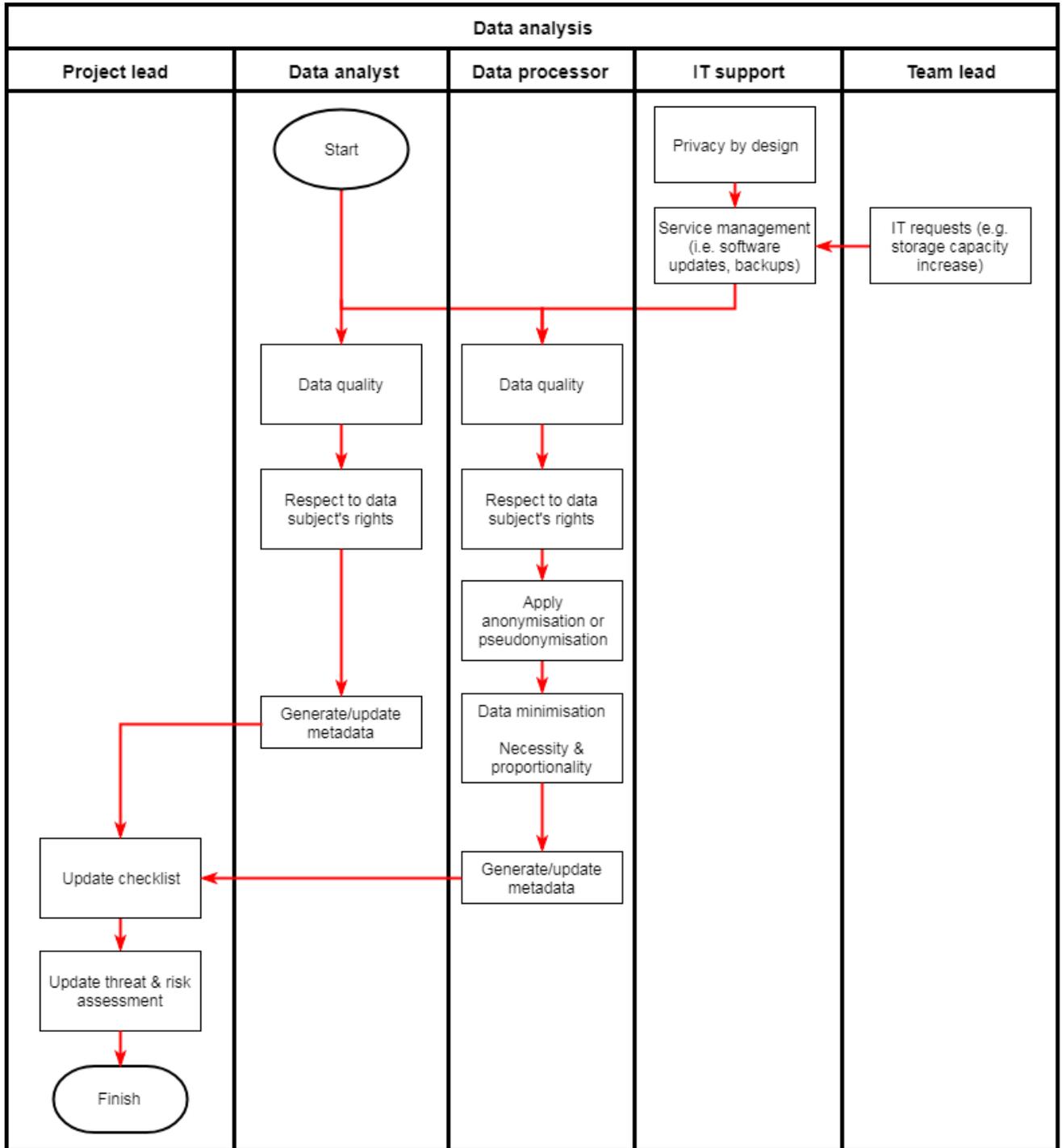
Stage Collection & Access



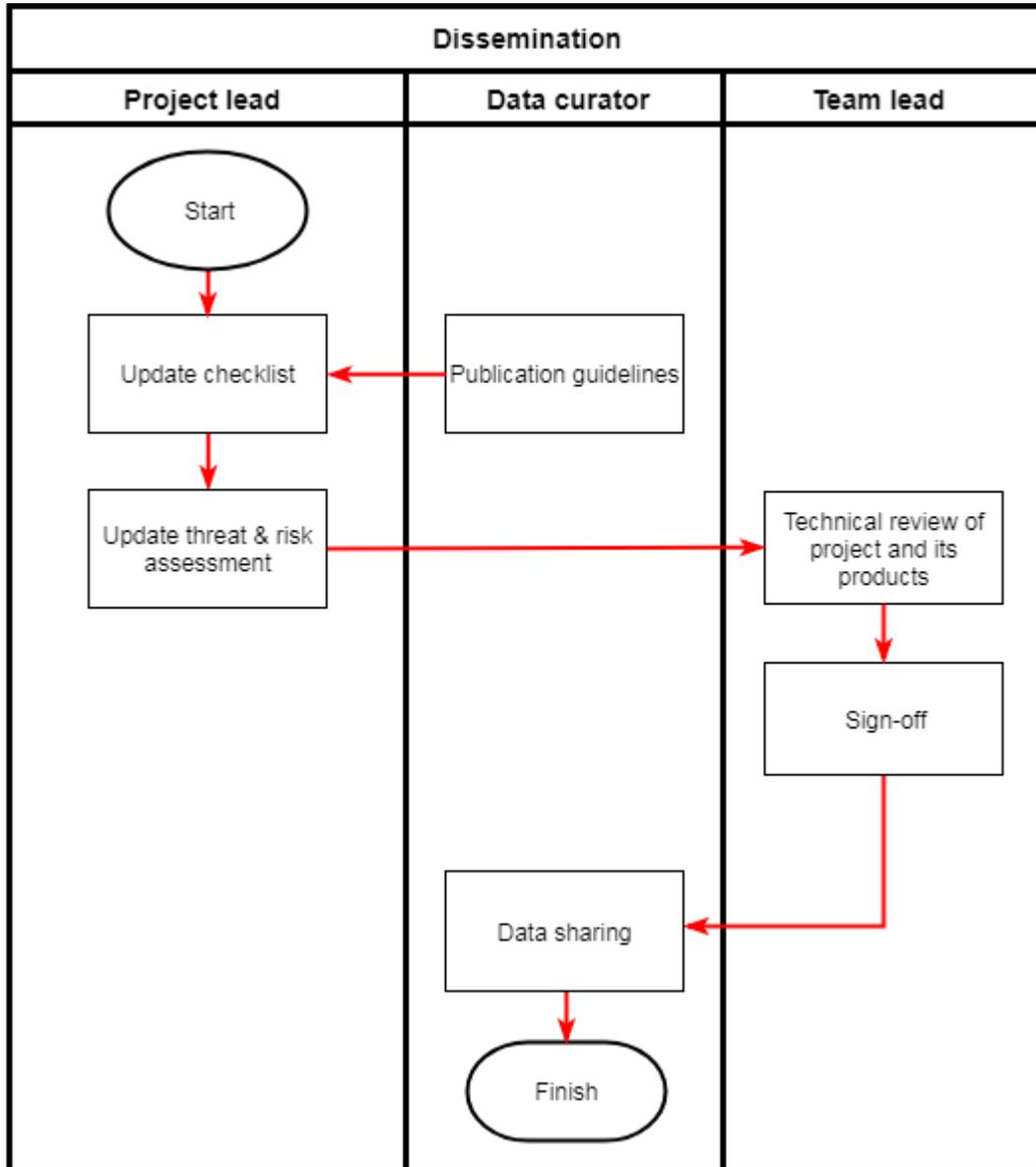
Stage Transportation & Storage



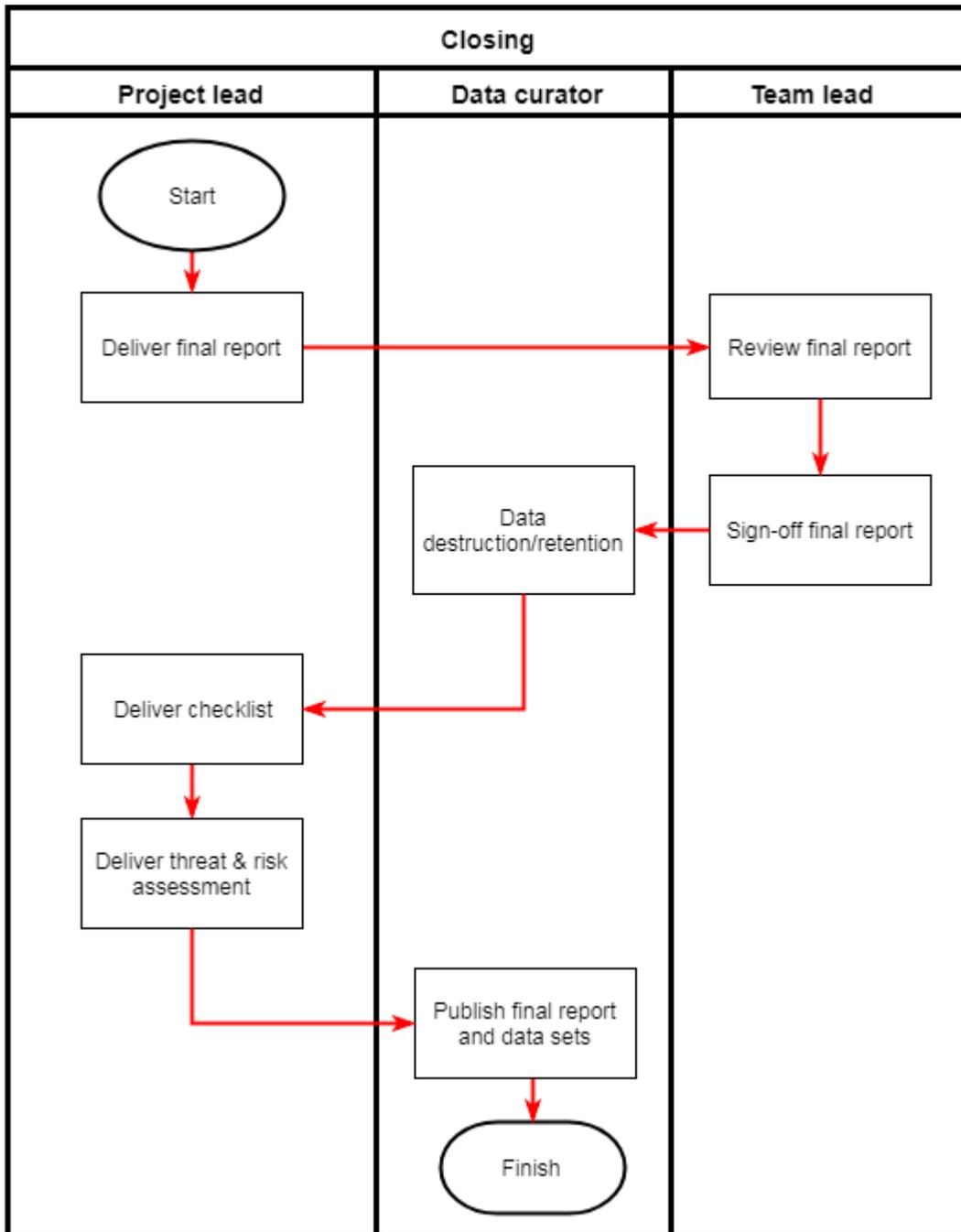
Stage Data analysis



Stage Dissemination



Stage Closing



E. Registration form template for processing personal data

Use this template to register the details for processing personal data.

(An English version is being prepared, the Dutch version can be found on NLRC's Intranet)

F. Methods anonymisation and pseudonymisation

| Method: | Scheme: | Original entry: | After method: | | | | | | | | |
|---|--|---|--|--------------|---------------|---|---|-------------------|----------|-------------|----------|
| Anonymisation | Deletion | John Doe | - | | | | | | | | |
| | Aggregation | Age entries: 52, 20, 18 | Average of ages: 30 | | | | | | | | |
| | Conversion | Birth: 10-Jan-1985 | Age: 33 years (from 2018) | | | | | | | | |
| Pseudonymisation | Obfuscation a.k.a. masking. The key  used to reveal the masked info is kept separately from the data. | +31-10-1234567 | +31-##-##### | | | | | | | | |
| | Replace identical entries with identical masked info a.k.a. pseudonyms. | <table border="1"> <tr><td>A. Doyle</td></tr> <tr><td>B. Christie</td></tr> <tr><td>A. Doyle</td></tr> </table> | A. Doyle | B. Christie | A. Doyle | <table border="1"> <tr><td>Tim Cook</td></tr> <tr><td>Heather Davis</td></tr> <tr><td>Tim Cook</td></tr> </table> | Tim Cook | Heather Davis | Tim Cook | | |
| | A. Doyle | | | | | | | | | | |
| B. Christie | | | | | | | | | | | |
| A. Doyle | | | | | | | | | | | |
| Tim Cook | | | | | | | | | | | |
| Heather Davis | | | | | | | | | | | |
| Tim Cook | | | | | | | | | | | |
| User-defined masking format applied with aid of key | <table border="1"> <tr><td>John Doe</td></tr> </table> | John Doe | <table border="1"> <tr><td>001_ID_1</td></tr> </table> | 001_ID_1 | | | | | | | |
| John Doe | | | | | | | | | | | |
| 001_ID_1 | | | | | | | | | | | |
| Encryption/de-cryption | Use of encryption key and algorithm to scramble Personal Data or DII. Use of decryption key  required to view and identify Personal Data or DII again. Note: Encrypted data cannot be processed. | <table border="1"> <tr><td><i>Encrypted:</i></td></tr> <tr><td>eFg#8xZ15nmo</td></tr> <tr><td>atH#2#xV25zXb</td></tr> <tr><td>eFg#8xZ15nmo</td></tr> </table> | <i>Encrypted:</i> | eFg#8xZ15nmo | atH#2#xV25zXb | eFg#8xZ15nmo |  <table border="1"> <tr><td><i>Decrypted:</i></td></tr> <tr><td>A. Doyle</td></tr> <tr><td>B. Christie</td></tr> <tr><td>A. Doyle</td></tr> </table> | <i>Decrypted:</i> | A. Doyle | B. Christie | A. Doyle |
| <i>Encrypted:</i> | | | | | | | | | | | |
| eFg#8xZ15nmo | | | | | | | | | | | |
| atH#2#xV25zXb | | | | | | | | | | | |
| eFg#8xZ15nmo | | | | | | | | | | | |
| <i>Decrypted:</i> | | | | | | | | | | | |
| A. Doyle | | | | | | | | | | | |
| B. Christie | | | | | | | | | | | |
| A. Doyle | | | | | | | | | | | |
| Pseudonymisation with encryption/de-cryption | Replace identical entries with identical masked info. Use of decryption key  required to view and identify Personal Data or DII again. Note: Encrypted data can be processed. | <table border="1"> <tr><td><i>Encrypted:</i></td></tr> <tr><td>Tim Cook</td></tr> <tr><td>Heather Davis</td></tr> <tr><td>Tim Cook</td></tr> </table> | <i>Encrypted:</i> | Tim Cook | Heather Davis | Tim Cook |  <table border="1"> <tr><td><i>Decrypted:</i></td></tr> <tr><td>A. Doyle</td></tr> <tr><td>B. Christie</td></tr> <tr><td>A. Doyle</td></tr> </table> | <i>Decrypted:</i> | A. Doyle | B. Christie | A. Doyle |
| <i>Encrypted:</i> | | | | | | | | | | | |
| Tim Cook | | | | | | | | | | | |
| Heather Davis | | | | | | | | | | | |
| Tim Cook | | | | | | | | | | | |
| <i>Decrypted:</i> | | | | | | | | | | | |
| A. Doyle | | | | | | | | | | | |
| B. Christie | | | | | | | | | | | |
| A. Doyle | | | | | | | | | | | |

G. Checklist template

Using this template you can capture your responses for the various steps in each stage of the data life cycle.



H. Threat and risk assessment template

Some general guidance for a threat and risk assessment in qualitative terms:



I. Third party data sharing agreement template

A template that can be used as a basis for data sharing:



It is accompanied by two additional templates:

(a) general declaration of consent template



(b) declaration of consent template for the use of visual materials



J. 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".

K. Data collection tools

| Kobo Toolbox | |
|---|--|
| <ul style="list-style-type: none"> Purpose of tool | <ul style="list-style-type: none"> KoBo Toolbox is a free open-source tool for mobile data collection, available to all. Enabling collection of data in the field using mobile devices such as mobile phones or tablets, as well as with paper or computers. |
| <ul style="list-style-type: none"> Source (e.g. for downloading of tool, FAQ etc) | <p>https://www.humanitarianresponse.info/en/applications/kobotoolbox</p> |
| <ul style="list-style-type: none"> Used in which stage(s) of the data life cycle (e.g. data collection & access, transport & storage, processing & analysis, dissemination) | <p>Data collection, Data transport and storage, Data processing & analysis.</p> |
| <ul style="list-style-type: none"> Specifics of data protection mechanisms or solutions when e.g. the data is collected in mobile phones and/or stored on a server. | <p>Main security features:</p> <p>In general: do not use this tool for Personal Data or DII without any form of data protection scheme. Forms can be encrypted using an encryption key and then sent to Kobo Toolbox for storage. The form can then be downloaded from the Kobo Toolbox on a smart phone. In order to see the form it needs to be decrypted using a decryption key. Decryption is achieved using ODK Briefcase. The whole procedure for encrypting and decrypting forms is possible, but cumbersome.</p> |
| <ul style="list-style-type: none"> Any best practices when using this tool | <p>Do NOT use Google drive or Dropbox if data can be linked to individuals. Workaround, before uploading: delete any personal data, apply pseudonymisation to personal data (e.g. masking of entries, swapping of entries, adding random numbers to numeric values) etc. Apply good password management, change passwords frequently, etc.</p> |
| <ul style="list-style-type: none"> Other specifics of tool worth mentioning (e.g. any scripts, templates or procedures that were developed by team to be used with the tool, etc) | <p>Setting up a link between google docs and Kobo: https://drive.google.com/file/d/1gcspFaPtLMpPLCii0t7cn9-KMzXvmxYi/view</p> |

| Mega V | |
|---|---|
| <ul style="list-style-type: none"> • Purpose of tool | Software for registration and humanitarian assistance distribution developed by the Mexican Red Cross to speed up review of beneficiary cards by using bar codes. |
| <ul style="list-style-type: none"> • Source (e.g. for downloading of tool, FAQ etc) | http://www.livelihoodscentre.org/-/mega-v-software-for-registration-and-humanitarian-assistance-distribution# |
| <ul style="list-style-type: none"> • Used in which stage(s) of the data life cycle (e.g. data collection & access, transport & storage, processing & analysis, dissemination) | Data collection, Data transport and storage, Data processing & analysis. |
| <ul style="list-style-type: none"> • Specifics of data protection mechanisms or solutions when e.g. the data is collected in mobile phones and/or stored on a server. | <p>Main security features:</p> <p>No specific data protection method(s) is/are mentioned as part of installing or using the Mega V software.</p> <p>The current implementation of Mega V software is meant to be run on a standalone laptop. In a future implementation where the tool would be run on a central database, data protection methods for storage and transport of Personal Data (e.g. encryption, password protection etc) would be possible.</p> |
| <ul style="list-style-type: none"> • Any best practices when using this tool | N/A |
| <ul style="list-style-type: none"> • Other specifics of tool worth mentioning (e.g. any scripts, templates or procedures that were developed by team to be used with the tool, etc) | N/A |

| MAGPI | |
|---|---|
| <ul style="list-style-type: none"> Purpose of tool | <p>It is a collection of tools that allow 1. collecting data through mobile devices, 2. sending them to an online server even if there is no internet connection or access to a mobile network at the time the data is collected, 3. designing online forms and 4. generating reports based on stored data.</p> |
| <ul style="list-style-type: none"> Source (e.g. for downloading of tool, FAQ etc) | <p>http://www.magpi.com</p> |
| <ul style="list-style-type: none"> Used in which stage(s) of the data life cycle (e.g. data collection & access, transport & storage, processing & analysis, dissemination) | <p>Data collection, Data transport and storage, Data processing & analysis.</p> |
| <ul style="list-style-type: none"> Specifics of data protection mechanisms or solutions when e.g. the data is collected in mobile phones and/or stored on a server. | <p>Main security features: The Magpi website and client software are constantly being evaluated and hardened to enhance security and protect against attacks.</p> <ul style="list-style-type: none"> • Full-device encryption can be accomplished on Android, and iPhone platforms using the built-in tools for each of those platforms (this process takes one minute on an iPhone). • Magpi is designed so that each user logs in with their own, unique userid and password. • Although most Magpi users use the internet (e.g. GPRS, 3G, Wi-Fi, etc.) to download forms to mobile devices and to upload data, it is possible to enter data from any phone via SMS, or to upload Symbian SMS app data or to send information via SMS. In these cases, data are not encrypted, and is therefore the least secure way to transmit information. • Public files are only viewable to people who have a link to the files. • Magpi uses Rackspace Cloud Storage for data storage, which has a robust security policy of its own. • Magpi uses modern encryption methods to transfer your data, including Secure Sockets Layer (SSL) and AES-256 bit encryption (with the exception of data transmitted by SMS). |
| <ul style="list-style-type: none"> Any best practices when using this tool | <p>N/A</p> |
| <ul style="list-style-type: none"> Other specifics of tool worth mentioning (e.g. any scripts, templates or procedures that were developed by team to be used with the tool, etc) | <p>N/A</p> |

| POSM | |
|---|---|
| <ul style="list-style-type: none"> • Purpose of tool | <p>Portable OpenStreetMap or “POSM” is a project to bring together assorted OpenStreetMap tools onto a portable device which works without an internet connection. POSM is being developed by the American Red Cross with humanitarian field mapping in mind.</p> |
| <ul style="list-style-type: none"> • Source (e.g. for downloading of tool, FAQ etc) | <p>https://github.com/posm/posm</p> |
| <ul style="list-style-type: none"> • Used in which stage(s) of the data life cycle (e.g. data collection & access, transport & storage, processing & analysis, dissemination) | <p>Data collection, Data transport and storage</p> |
| <ul style="list-style-type: none"> • Specifics of data protection mechanisms or solutions when e.g. the data is collected in mobile phones and/or stored on a server. | <p>Main security features:</p> <ul style="list-style-type: none"> • Password management is applied to login to device. • Data is not encrypted prior to uploading to device. • Hard disk of device is not encrypted. • WiFi link between smart phone and POSM is not secured. • The use of Secure FTP (S-FTP) may be possible, but has not been implemented yet. |
| <ul style="list-style-type: none"> • Any best practices when using this tool | <p>N/A</p> |
| <ul style="list-style-type: none"> • Other specifics of tool worth mentioning (e.g. any scripts, templates or procedures that were developed by team to be used with the tool, etc) | <p>N/A</p> |

L. Data storage options

GeoNode

GeoNode is an open-source geospatial content management system, a web-based application and platform enabling organisations to create data catalogues and allowing users to access, manage, share, and publish geospatial data. GeoNode has been successfully deployed in several regions to aid with disaster preparedness and emergency relief.

When dealing with exchange and publication of humanitarian related data, data sensitivity needs to be guaranteed. GeoNode implements a framework of users, groups, and permissions to address this:

1. Every user can access and potentially edit only data which she/he is allowed to see and manage.
2. The user who uploads data becomes its owner on the platform and can assign permissions to other users and groups.
3. The system administrator has always the possibility of making changes to the permissions in case of need.

HDX (Humanitarian Data eXchange)

The Humanitarian Data Exchange ([HDX](#)) is an open platform for sharing data, launched in July 2014. The goal of HDX is to make humanitarian data easy to find and use for analysis.

Anyone can view and download the data from the site, but registered users can access more features such as: following the latest changes to data, locations, organisations, topics and crises, sharing datasets (or only metadata) publicly or privately, getting access to private datasets, etc.

All data shared publicly through the platform must be sufficiently aggregated or anonymised so as to prevent identification of people or harm to affected people and the humanitarian community. All data on HDX must include a minimum set of metadata fields.

Microsoft Azure

Microsoft Azure is a collection of services that enables users and organisations to create, deploy, and operate cloud-based applications and infrastructure services.

It provides software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS) and supports many different programming languages, tools and frameworks, including both Microsoft-specific and third party software and systems.

Cloud storage providers (such as Microsoft) can host your data in the EU.

MS Teams

In MS Azure the tool MS Teams is used for data storage, data search & retrieval and communications.

Files can be stored within a channel in a hierarchical structure of folders and sub-folders. There are no options for using/assigning metadata fields to a document. It is recommended to use an appropriate and consistent file naming convention, which is useful for understanding and retrieving of the file, e.g:

[dd_mm_yyyy]_[Name_Of_File]_[Initials of User]_[version_x_y].[extension]

Example: 21_05_2018_Data_Storage_Classifiers_JB_version_0_1.doc

Per channel only collective access permissions can be assigned to team members within a specific team: either all team members can access the data, or none of them can. A so-called Role Based Access Control (RBAC) scheme enabling some team members to have “read-only rights”, while others have “editing rights” or “full control rights” based on their team role, is not possible in the current version of MS Teams. Creation of top-level channels, and initial assigning of team members to those channels with specific permissions e.g. for creating/updating/deleting channels, is done by the Team leads.

Communications in the form of chats can take place using either public channels, or private channels. Skype for Business can be used for audio and/or video conferencing and requires a user name and password associated with a business account.

Using a mobile version of the tool, enables users to receive notifications of changes to files, access to channels, etc.

MS Planner

The tool MS Planner is used for defining, scheduling and assigning of project tasks to team members. The contents of MS Planner and MS Teams can be linked, so that users can easily navigate between tasks, channels and files without the need of duplicating files across these tools. The files are actually stored on SharePoint/OneDrive, which is all part of the Microsoft Cloud, just like Azure.

M. Basic metadata template

A basic metadata template that may be used to capture several initial properties of a dataset. This file should have the exact same name as the dataset with `_METADATA` added at the end and saving it as an .xlsx file or a .txt file.



N. Preferred IT platform according to functional requirement

This section is left blank intentionally. For more details, please contact 510.

O. Creative Commons Licenses

Source : <https://creativecommons.org/licenses/>

| License type | Explanation | Symbol |
|---|---|---|
| Attribution CC BY | This license lets others distribute, remix, tweak, and build upon your work, even commercially, as long as they credit you for the original creation. This is the most accommodating of licenses offered. Recommended for maximum dissemination and use of licensed materials. |  |
| Attribution-ShareAlike CC BY-SA | This license lets others remix, tweak, and build upon your work even for commercial purposes, as long as they credit you and license their new creations under the identical terms. This license is often compared to “copyleft” free and open source software licenses. All new works based on yours will carry the same license, so any derivatives will also allow commercial use. This is the license used by Wikipedia, and is recommended for materials that would benefit from incorporating content from Wikipedia and similarly licensed projects. |  |
| Attribution-NoDerivs CC BY-ND | This license allows for redistribution, commercial and non-commercial, as long as it is passed along unchanged and in whole, with credit to you. |  |
| Attribution-NonCommercial CC BY-NC | This license lets others remix, tweak, and build upon your work non-commercially, and although their new works must also acknowledge you and be non-commercial, they don't have to license their derivative works on the same terms. |  |
| Attribution-NonCommercial-ShareAlike CC BY-NC-SA | This license lets others remix, tweak, and build upon your work non-commercially, as long as they credit you and license their new creations under the identical terms. |  |
| Attribution-NonCommercial-NoDerivs CC BY-NC-ND | This license is the most restrictive of our six main licenses, only allowing others to download your works and share them with others as long as they credit you, but they can't change them in any way or use them commercially. |  |

P. Data breach procedure

A security breach is said to have occurred when personal data have been found in a place where they are not supposed to be. A security breach can occur when for example:

- Your laptop, mobile phone or a paper file with personal data has been lost or stolen;
- You have shared information containing personal data with someone who is not authorized to have access to that data, for example when an e-mail was sent to the wrong recipient;
- You inadvertently have unauthorized access to confidential information;
- You find confidential information in a place where it is not supposed to be stored;
- You open a link or an attachment associated with a suspicious e-mail;
- Your computer or mobile phone has been hacked or infected with a virus.

A security breach shall be reported to your line manager and the information manager of your cluster within 24 hours of its occurrence.

An investigation will take place to determine if a data breach occurred and, if needed, what adequate measures to take.

Should you have any questions or remarks, please refer to the site "Privacy en Informatiebeveiliging" on the Intranet, or send an e-mail to privacy@redcross.nl