Protection Policy

# Preamble

Spatial data and mapping activities have the potential to create risk or cause harm to people and communities. HOT, as an agency both carrying out and supporting mapping activities and creating open, freely available spatial data with few constraints on its use, is responsible to understand, assess, mitigate, and protect against risk and harm arising from activities we undertake or support.

This policy lays out the ways in which stakeholders in data collection activities, data storage, and data use can approach these responsibilities, and represents HOT’s commitment to responsible, ethical practices to protect people from harm.

# Application and Practicality (light touch)

This document is not intended to create obstacles to normal work or add bureaucracy. Most people within HOT and associated communities and stakeholders should be aware of its existence, but not have any need to consult it during day-to-day activities and routine projects.

However, Senior Management Team members as well as project managers dealing with risky contexts or activities as defined, are expected to be familiar with this document, and be aware of the circumstances in which activities, projects, and data must be assessed for potential harm.

It is essential that when anyone within the organization is concerned about Protection risk, this document, and the guidance and tools that support it, must be discoverable and available to them. Furthermore, in any case where Protection risk is likely to arise (such as mapping in conflict zones), the Director(s) responsible for the projects are responsible for ensuring that this policy is consulted.

# Definition and scope

The word Protection is used here in a way similar to its [common usage in the humanitarian field](https://www.unocha.org/es/themes/protection), which encompasses two basic definitions:

1. Protect the lives, livelihoods and dignity of affected people, and
2. Ensure that our own actions do not lead to or perpetuate discrimination, abuse, neglect or violence.

In humanitarian or conflict settings, both definitions apply. However, in peaceful, stable development contexts (as opposed to humanitarian or conflict settings), the overwhelming emphasis is on definition 2, which can be summarized by the common injunction, “*First, do no harm.*[[1]](#footnote-0)”

## In scope:

* Mitigation planning to reduce the risk of harm to people and communities being mapped (as opposed to staff and mappers) from:
  + Activities undertaken directly by HOT
  + Activities undertaken by others (communities, partners etc) with *direct* support from HOT (financing, material, or in-kind support)
  + Activities undertaken using HOT’s own managed infrastructure (Tasking Manager or similar)
  + Data owned and managed by HOT
  + Data owned and managed by others that was directly derived from HOT-supported activities
  + Creation of data (Open Data or not) that a duly diligent assessment would find creates risk and/or harm to people or communities

## Out of scope:

* Operational safety and security. This document’s focus is impact and risk on communities being mapped, not the safety and security of mappers. Safety and security are important, and overlap somewhat with protection, but are ultimately a separate concern.
* Risk of harm from
  + Use by others of [Free and Open Source Software](https://en.wikipedia.org/wiki/Free_and_open-source_software) (FOSS) created or supported by HOT (as opposed to using HOT’s own infrastructure).
    - For example, if another organization creates their own instance of the Tasking Manager, without direct support from HOT, use of HOT logos, or direct involvement from HOT, the principles of FOSS and the Tasking Manager license[[2]](#footnote-1) are clear: anyone is free to use the software, and HOT is not responsible for their conduct.
  + Use by others of [Open Data](https://en.wikipedia.org/wiki/Open_data) created or supported by HOT.
    - For example, use of OpenStreetMap data is governed by the [Open Database License](https://opendatacommons.org/licenses/odbl/), which allows any use whatsoever provided the data is attributed, shared, and kept open. HOT (or any other creator of such Open Data) is not responsible for the conduct of users.
* However, the *creation of Open Data that may cause harm* remains firmly within the scope of this policy. In a sense, once released into the world, Open Data cannot be recalled. Therefore its creation and release carries responsibilities.Information security and IT practices. While Protection implies a responsibility to properly secure sensitive data (sometimes referred to as Data Protection[[3]](#footnote-2)), this document does not prescribe how this is to be done.
  + For example, questions of how to secure passwords for Quickbooks, set permissions in Google Drive, or use 2FA on email accounts is the responsibility of the Data Security team at HOT. Questions of *what data we should even consider having, keeping on Google Drive or internal storage, or sending by email*, based on the potential of such data to cause harm, fall within the scope of this document.

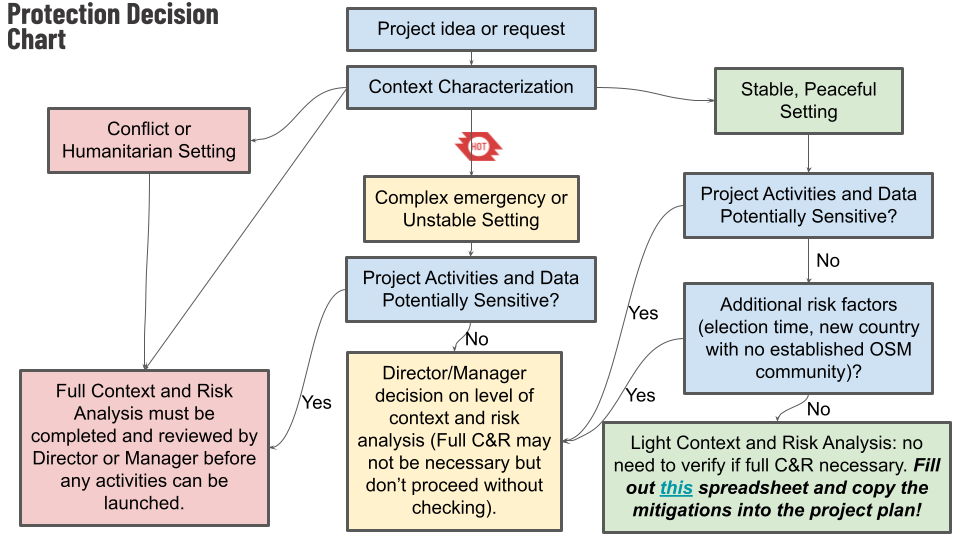
# 

# Required Steps Before Starting Open Mapping Projects

* ***All Open Mapping projects with a field component require a Protection Risk assessment.***
* ***All “Activations” require a Protection Risk Assessment as part of the size-up.***
* ***Some Tasking Manager–based remote mapping projects (primarily those in identified high-risk and/or high-sensitivity zones) require a Protection Risk Assessment.***

However, in many cases, the Protection Risk Assessment may be a very light process; this policy is not intended to impede or inconvenience “business as usual” Open Mapping.

For example, the path to the green box on the lower right of this flowchart leads to a requirement of only a simple spreadsheet-based Protection Risk Assessment exercise that should take no more than an hour.



There are three categories of project, corresponding to the bottom boxes in the flowchart.

* **Green**: Light Context and Risk analysis required. A [simple spreadsheet exercise](https://docs.google.com/spreadsheets/d/15HWx3R_K_FT-9nBA3FUxEaxhi6Q7nXMt1py0tFdTnG8/edit#gid=668561724) is done by the project owner (which may be a community grantee, their mentor,
* **Yellow**: Medium or Uncertain, Director/Manager decision on level of assessment required
* **Red**: Equivalent to conflict zone and/or highly sensitive data collection; automatically requires full context and risk analysis and Director-level approval to begin activities.

The types of Risk Assessments are the following:

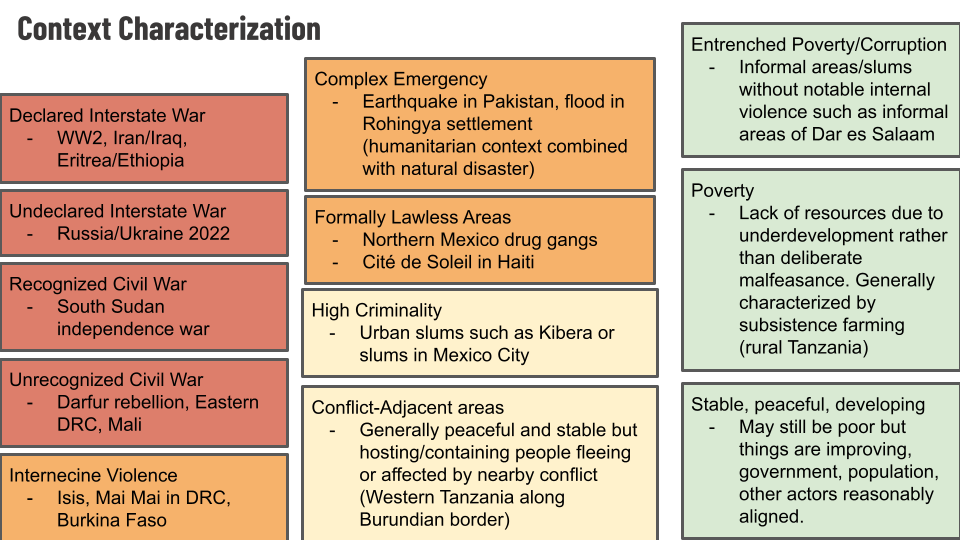
* Light Context and Risk Analysis
  + Who can approve it - the project manager, or Director/Team Lead
* Full Context and Risk Analysis

Any Risk Analysis levels asses three components which are explained below:

* Context Characterization
  + The outcome
* Other contextual factors
* Sensitive data

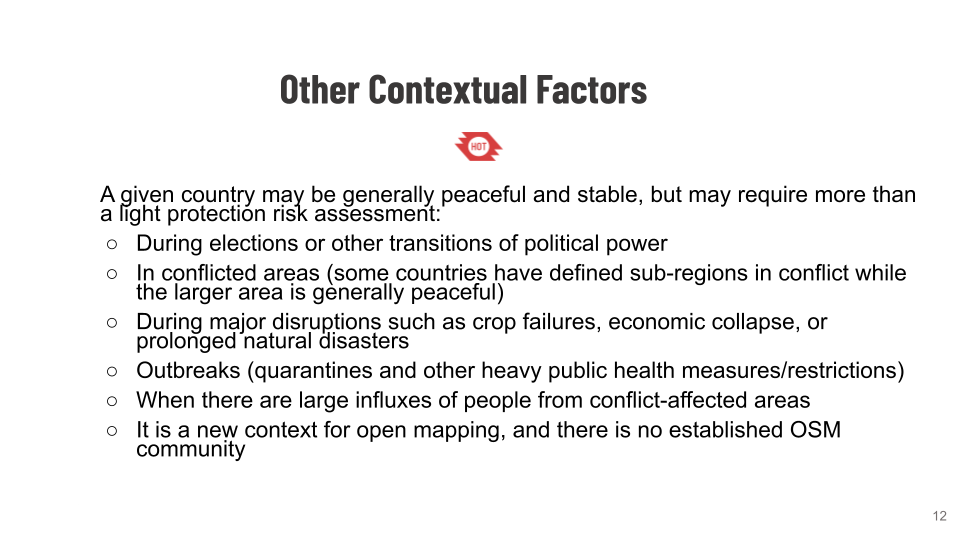
## Context Characterization

In order to keep this policy from becoming an obstacle or dead weight, it must be straightforward to identify situations where “business as usual” is probably fine.

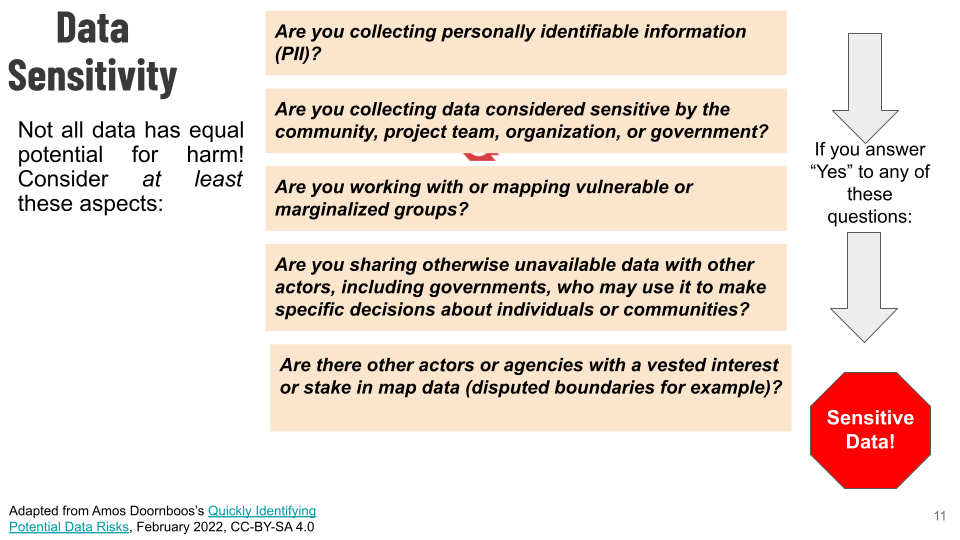


This chart, with examples of contexts that may be familiar (or at least easy to look up) is intended to help guide project owners to determine whether they are in context that automatically requires a Yellow or Red level of Protection Risk assessment.

## Additional criteria: other contextual factors



## Additional criteria: sensitive data



## Risk Assessment Template

[This spreadsheet](https://docs.google.com/spreadsheets/d/15HWx3R_K_FT-9nBA3FUxEaxhi6Q7nXMt1py0tFdTnG8/edit?usp=sharing) is the basic template/tool for Protection Risk Assessment. It follows the classic Vulnerability/Likelihood/Impact logic of many Risk Assessment tools, but is specifically intended for application to Protection risk (risk to communities) as opposed to Operational Safety and Security (risk to mappers).

### Due Diligence

Impact assessments must be conducted to a credible standard. “We didn’t realize it was dangerous for people” is not an excuse for causing harm if we haven’t deployed credible effort and expertise to determine if there’s danger. Broadly speaking you have exercised [Due Diligence](https://jusmundi.com/en/document/wiki/en-due-diligence-1) if you meet all the following criteria:

* You’ve met or exceeded normal industry standards and practices
* You’ve done everything that a reasonable external observer would expect you to do to prevent harm
* You have sufficient expertise—or have consulted with those possessing sufficient expertise—to determine what risks of harm are involved in your activities in the specific context you are operating.
* You’ve followed all applicable laws

## Mitigation

1. From the Latin [*Primum non nocere*](https://en.wikipedia.org/wiki/Primum_non_nocere), a principle in both humanitarian and development work borrowed from the health field, which, as per the article in the link above, is “invoked when debating the use of an intervention that carries an obvious risk of harm but a less certain chance of benefit.” [↑](#footnote-ref-0)
2. [HOT’s Tasking Manager is licensed under a BSD 2-Clause license](https://github.com/hotosm/tasking-manager/blob/develop/LICENSE.txt), a liberal (non-copyleft) license that permits any use whatsoever of the code provided the copyright notice, conditions, disclaimer, and source code are made available with any distribution. [↑](#footnote-ref-1)
3. Though this is a narrow and incomplete definition; a more complete definition of [Data Protection is better phrased as Information Privacy](https://en.wikipedia.org/wiki/Information_privacy) and addresses questions of what data to have/create, not merely how to technically secure it. [↑](#footnote-ref-2)