Norwegian People's Aid

Digital security for partners

Consultancy

Terms of Reference

June 2022

1. Background

Civil society actors worldwide experience increasing threats and a shrinking civic space. Strengthening partners security is therefore a prioritised area in NPA's Development and Humanitarian Cooperation (DHC) work in the coming years. People's physical organising remains the most efficient means of mobilisations, particularly for marginalised people, even if online public campaigns such as the ¨MeToo¨ movement have had a worldwide impact and been key for women mobilising in different countries. Increasingly the digital space provides both an important tool in peoples organising and arena where people actually meet.

Thus, at its best this digital space provides an arena for free expression and access to information, establishing and maintaining networks based on common interest and for campaigning and mobilizing around a cause. At its worst the digital space is extremely effective as means for surveillance, manipulation and repression.

Digital security is therefore closely linked to partners safety and ability to operate and organise effectively.

2. Purpose

The overall purpose of this initiative is to strengthen NPA's support partners to continue their work in a safe manner and achieve their objectives in contexts of high risk. Specifically, this initiative will contribute to enable NPA to support partners to take the adequate, realistic and relevant measures to protect their data and communication and prevent unauthorised access to data, thereby also protecting themselves and their organisation and supporters.

This consultancy will provide advice, analysis and information and support to implementation to enable NPA to achieving the overall purpose, as specified below.

3. Methodology

The consultant will:

- Undertake a mapping of relevant resource organisations, international, regional and local with mandate and scope to support civil society actors' digital security. The mapping will identify approach, strengths and weaknesses of the resource organisations and geographical reach.
- Map and document learning from existing NPA experiences with digital security support to partners.
- Outline options for NPAs engagement to support partners' digital security, looking at NPAs role, scope and limitations. The outline should include different options as to how digital security training for NPA staff and partners could be organised and how to guide our partner dialogue on digital security.
- Contribute to plan a digital risk assessment in selected countries identifying the main risk in NPA - partner relation.
- Contribute to plan support to partners to conduct digital risk assessment to identify the gaps and main risk areas of their organisations
- Coordinate a review of the pilot phase to inform further roll out

The tasks of the consultant will be developed in close coordination with NPAs country offices in the relevant countries as well as programme coordinators at head office. Particularly, the consultant will coordinate with NPAs IT and Security sections.

4. Expected Outputs from the consultancy

- A short document summarising existing NPA experiences of supporting partner digital security with main learning points.
- A mapping of relevant resource organisations, international, regional and local with mandate and scope to support civil society actors' digital security.
- Recommendations to NPA of relevant resource organisations
- A proposal for terms of collaboration with selected relevant resource organisations on digital security for civil society actors
- Recommendations on the scope and limitations of NPAs support to partners' digital security, including roles of different sections within NPA.
- Pilot digital risk assessment conducted for some selected partners.
- Pilot digital security training conducted for some selected partners.
- A review of the pilot phase to inform further roll out.

5. Timeline

The consultancy will initiate August 2022 and have a duration of 6 months with an estimated 18 hours per week.

6. Reporting

The consultant will report to the DHC management team (DHCMT), and managed by Beate Thoresen.

7. Qualifications

The consultant must have:

- Good understanding of digital security and risks for civil society organisations.
- Good communication skills and capacity to explain IT technology and digital security in understandable terms.
- Work experience from security management, hereunder particularly with focus on digital security.
- Good overview of civil society networks working with digital security internationally is an advantage.
- Excellent communication skills in English required, other languages an advantage.