Annex 12 Security Plan

On September 27, 2020, the Azerbaijan - supported by the Turkish military and Syrian mercenaries - started large scale military offence against the unrecognized Republic of Nagorny Karabakh. The 44 day-long armed conflict ended up with a Russian-brokered cease-fire on November 9, 2020, causing huge devastation to the region, left thousands dead, many settlements ruined, and a part of NK proper under Azerbaijani control. During the 44 days of armed conflict it was not safe to travel to the South of Armenia. As post-conflict demarcation of borders is not complete yet, South of Armenia remains a region of high security risk.

After the Velvet Revolution Armenia made progress in Internet freedom[1] reflected in Freedom House reports, at the same time a rise of hate speech and verbal assault is also recorded. Generally, civil society organizations are operating in relatively safe environment, however outspoken LGBT and feminist groups as well as human rights defenders are a subject to severe verbal attacks, predominantly online.[2] In 2019 one of the groups engaged in promulgation of anti-democratic values called 'Veto' for three consecutive weeks was blocking an entrance to the Open Society Foundations-Armenia, after the 44-day armed conflict there were attacks on Radio Free Europe, OSF and some activists. There were also verbal attacks on EPF and its employees.

Post-conflict internal situation in the country remains tense. Anti-liberal, anti-democratic large-scale propaganda – both home grown and foreign baked- as well as unprecedentedly aggressive misinformation campaign is going on against various groups, especially against human rights defenders and peacebuilding community are at the target. On top of previous allegations, some activists are named 'traitors that have to be punished', foreign agents and 'spies of the enemy'. Among online verbal attacks trolling, dissemination of fake news, labelling and abusive media articles may be anticipated. From cyber-security perspective fishing of data, DDOS and virus attacks can be initiated.

In addition to the conflict, COVID-19 and imposed limitations, also impacted the overall security situation in the country. During the COVID-19-imposed lockdown (from April to July 2020), the activities under the "Partnership for Justice Reform" project were conducted on online working mode, which provided an opportunity to EPF and the Consortium members to conduct on-line discussions, training, involving also some stakeholders. Even after the post-pandemic period, EPF and its partners believe this modality of having joint online events/discussions, and trainings will also continue.

[1] https://freedomhouse.org/report/freedom-net/2018/armenia
[2] https://www.frontlinedefenders.org/en/location/armenia

The physical security of EPF premises is ensured through CCTV system and 24/7 security assurance. In compliance with EPF's policies and procedures, there is also a property insurance which covers physical damage to the space and equipment. EPF also has alarm system and will establish contact with the hot line of the Police covering the area. EPF will make sure that risky meetings are organized in safe spaces which already have security systems such as hotels, business centers, etc. As a part of DRL funded Partnership for Justice Reform project, EPF hired a team of psychologists who work with staff and partners providing counselling and support. The psychological assistance will be extended to other members of the team if needed.

EPF will share its Emergency Preparedness Plan (*Annex 18_EPF Emergency Preparedness Plan*), Incident Management Plan (*Annex 19_EPF Incident Management Plan*) and IT security and communication rules, which are part of EPF's Policies and Procedures (*Annex 17_EPF Armenia P&P Manual*), with other members of the Consortium.

The security plan of the project will anticipate the following activities:

1. For EPF staff travel to South of Armenia will be restricted and allowed only with written permission of the CEO.

2. VPNs were set up for EPF, the messages are stored on ProtonMail servers in encrypted format. Secure implementations of AES, RSA, along with OpenPGP are used. The annual service fee of the VPNs will be needed. EPF will provide additional VPN's to grantees and partners upon request.

3. Selection of the Facebook as a platform for online coordination/communication is determined not only by its large-scale usage but also security reasons. Facebook is more secure than any application developed and maintained locally. However, pro-bono online and cyber security trainings will be provided for partners and grantees.

4. Zoom platform is used for the online discussions and trainings. Security measures will be taken to ensure that personal data is protected, including setting passwords for all meetings and ensuring communication rules.

5. EPF will hire a high-level IT and cyber-security consultant for the entire course of the project. The consultant will be responsible for ensuring IT and online security at the workplace and beyond for all Consortia members.

6. EPF will update its communications and public outreach strategies, taking into consideration recent cyber and physical attack risks.