Support to Digital Defenders Partnership (DDP) for 2020-2022

Key results:

- Human Rights Defenders (HRDs) remain resilient to closing civic space and continue to effectively use the Internet and Information and Communications Technology to promote and defend human rights

- HRDs have access to strengthened global and regional organisations, networks and individuals providing digital security, protection and digital rights support to civil society.

- Accessible, collaborative, resilient and responsive networks of expertise and support for HRD organisations, individuals or networks under digital threat are developed and strengthened

Justification for support:

- The development of an independent and diverse civil society is fundamental in promoting democracy and delivering on the Sustainable Development Goals.

- Promoting space for civil society is a priority for Denmark's as part of the initiative #DK4CivicSpace. DDP is contributing to this end by enhancing the resilience of civil society organisations, human rights defenders, activists etc. facing digital attacks on their freedoms of expression, assembly and association.

Major risks and challenges:

- HRDs, organisations, networks or recipients of DDP funding are endangered by being linked to (activities/funding of) the DDP.

- Specific threats to staff of local organisation (raid, account hacking, detention) and/or regional trainers (arrest, detention, torture, accidents).

- Governments preventing HRD's organisations or networks from being supported.

- Regional trainers not being able to enter a country to support local HRDs, organisations or networks.

File No.	2019- 27991					
Country	Interregional					
Responsible Unit	HCE					
Sector	15150 Democratic participation and civil society					
Partner	Digital Defenders Partnership					
DKK mill.	**2020**	**2021**	**2022**	**20xx**	**20xx**	**Tot.**
Commitment	11.25					11.25
Projected ann. disb.	3.75	3.75	3.75			11.25
Duration	2020-2022 (36 months)					
Previous grants	N/A					
Finance Act code	06.32.08.70					
Head of unit	Mette Thygesen					
Desk officer	Adwan Mohamad					
Reviewed by CFO	Jacob Strange-Thomsen					

Relevant SDGs *[Maximum 1 – highlight with grey]*

No Poverty	No Hunger	Good Health, Wellbeing	Quality Education	Gender Equality	Clean Water, Sanitation
Affordable Clean Energy	Decent Jobs, Econ. Growth	Industry, Innovation, Infrastructure	Reduced Inequalities	Sustainable Cities, Communities	Responsible Consumption & Production
Climate Action	Life below Water	Life on Land	Peace & Justice, strong Inst.	Partnerships for Goals	

Strategic objectives:

To strengthen the digital resilience of civil society actors enabling them to exercise their freedoms of expression, assembly and association.

Justification for choice of partner:

DDP was founded by the intergovernmental Freedom Online Coalition, to which Denmark has applied for membership, to protect critical internet users, to defend human rights, and keep the internet free and open. DDP applies a holistic approach to digital resilience by combining emergency response with long-term capacity building and also psycho-social support. DDP has global presence and a wide network in the digital rights community

Summary:

Surveillance, facial recognition, internet shutdowns and hacking of computers are examples of means being applied against civil society actors and human rights defenders in order to limit their operability. This is part of an overall trend of shrinking space for civil society. In this context, human rights defenders, activists, bloggers, civil society organisations, journalists etc. need concrete tools to defend themselves against digital threats and build digital resilience. DDP will provide emergency funding and capacity building for HRDs and organisations in order to enhance their digital resilience. Furthermore, DDP will provide assistance to develop and strengthen networks among civil society actors under threat.

Budget:

Incident Emergency Response	DKK 1,734,857
Sustainable Protection Support	DKK 7,318,359
Facilitate and Build Community	DKK 2,006,113
Contingencies and indirect costs	DKK 190,671
Total	**DKK 11,250,000**

Denmark's contribution to the Digital Defenders Partnership for 2020-2022

Development engagement document

1. Introduction

The present development engagement document details the objectives and management arrangements for the development cooperation concerning support to the Digital Defenders Partnership for 2020-2022 as agreed between the parties specified below.

1.1 Parties

Ministry of Foreign Affairs of Denmark (MFA), Department for Humanitarian Action, Civil Society and Engagement and Stichting HIVOS, Digital Defenders Partnership Programme (DDP).

1.2 Documentation

"The Documentation" refers to the partner documentation for the supported intervention, which is the Digital Defenders Partnership Proposal to Denmark and its annexes.

1.3 Contributions

Denmark, represented by Department for Humanitarian Action, Civil Society and Engagement of the Ministry of Foreign Affairs of Denmark, commits to a contribution to the engagement of DKK 11,250,000 (eleven million two hundred and fifty thousand) for the period 2020-2022.

2. Background

Digital technologies represents new opportunities and challenges for civil society organisation, human rights defenders and activists. On the positive side, online platforms and communication systems can be a powerful tool for campaigning and mobilisation as well as for giving voice to civil society.

At the same time, digital tools are also being applied as means for control with the purpose of limiting the freedom of expression as well as the freedom of assembly and association. The United Nations Special Rapporteur on the rights to freedom assembly and of association has in a report to the Human Rights Council (2019) pointed to various ways in with digital technologies are being used to challenge basic rights.

Surveillance and facial recognition is being used to deter human rights defenders, activists and civil society organisations from participating in peaceful protest. Internet shutdown, bandwidth throttling and denial of service is used to limit the operability of civil society actors – often in relation to peaceful protests and elections. Censorship and content regulation is being enforced on journalists, activists etc., thereby limiting the freedom of expression. Hacking of computers and phones to disseminate doctored content, spread conspiracy theories etc., is done with an intention to hamper the work of civil society actors. Often the most vulnerable groups such as LGBTI persons, indigenous peoples and women's groups are also most at risk.

These tendencies seem to be part of an overall trend of shrinking space for civil society. According to Freedom House, global internet freedom has been in decline for the last nine years. In this context, human rights defenders, activists, bloggers, civil society organisations, journalists etc. need concrete tools to defend themselves against digital threats and build digital resilience.

Digital Defenders Partnership (DDP) was founded in 2012 by the intergovernmental Freedom Online Coalition to protect critical internet users, to defend human rights and keep the internet free and open. DDP applies a holistic approach to digital resilience by combining emergency response with long-term capacity building and also psycho-social support. Furthermore, specific focus on gender and vulnerable groups is given through the Gender Equality and Diversity Inclusion Strategy. Denmark has in 2020 submitted an application for membership of Freedom Online Coalition.

DDP is hosted by the international development organisation Hivos with headquarters in The Hague and regional hubs in Harare, Jakarta, Nairobi and San José and country offices in Bolivia, Guatemala, Lebanon, South Africa, Tanzania, Timor-Leste and Zimbabwe. Furthermore, DDP has a wide network in the digital rights community including Access Now, Frontline Defenders, Lifeline to name a few.

DDP is working towards a vision of an open internet, free from threats to expression, association, assembly privacy and other human rights, specifically in repressive and transitional environments. In doing so, the overall objective of DDP's current strategy for 2020-2023 is that Human Rights Defenders remain resilient to closing civic space and continue to effectively use the internet and information and communications technology to promote and defend human rights. As part of its theory of change DDP is working to realize this objective through strengthening awareness and building capacities of civil society actors as well as developing collaborative networks among relevant stakeholders.

A diverse and thriving civil society is an essential element in delivering on the Sustainable Development Goals and in promoting democratization in general. Therefore, countering the shrinking of civic space is a priority in Denmark's strategy for development cooperation and humanitarian action. On the Danish Finance Act for 2020, the Danish Government has allocated funds for an overall initiative regarding civic space - #DK4CivicSpace. As part of this initiative special focus will be directed at enhancing the digital resilience of civil society organisations.

3. Development Engagement Objective

The objective of the development cooperation among the parties is for Human Rights Defenders (HRDs) to remain resilient to closing civic space and continue to effectively use the Internet and Information and Communications Technology to promote and defend human rights.

This contribution will provide support for DDP's activities in countries listed on the OECD DAC list of ODA recipient with special focus on priority countries for Denmark's development cooperation.

The MFA will base the actual support on progress attained in the implementation of the engagement as described in the documentation. Progress will be measured through the Digital Defenders Partnership's monitoring framework.

For MFA's reporting purposes the following key outcome and output indicators have been selected to document progress:

Project title		**Digital Defenders Partnership**	
Project objective		Human Rights Defenders (HRDs) remain resilient to closing civic space and continue to effectively use the Internet and Information and Communications Technology to promote and defend human rights	
Impact Indicator		Increased awareness and stronger global movements working for human rights from a digital perspective. Continued internet access despite blockages. Increased availability and use of secure and innovative technologies.	
Baseline	Year	2019	Participatory and desk research carried out in 2018-2019 as basis for the DDP current strategy.
Target	Year	2022	In 2021/2022 DDP will perform a mid-term evaluation over her 2020-2023 strategy period and impact towards these indicators will be taken with.
Outcome 1		HRD organisations, individuals or networks can prevent or recover from digital threats (including threats to digital rights) in high risk contexts	
Outcome indicator		% of HRD orgs, individuals (disaggregated by gender), organisations, and networks that sustained their human rights work after receiving DDP Incident Emergency Funding (IEF), Sustainable Protection Funding (SPF), Digital Integrity Fellowship (DIF) accompaniment, or engaging with resources. The extent to which HRDs indicate that DDP interventions effectively responded to threats faced. % of HRDs who receive support from DDP-supported Global and Regional Partner projects who indicate an improvement in their security capacities resulting from the support.	
Baseline	Year	2020	Qualitative data based on applications for emergency support received. Long-term indicators set by recipients of Digital Integrity Fellowship accompaniment at beginning of projects. Long-term indicators set by recipients of Sustainable Protection Funding in application. Long-term indicators set by recipients of Global and Regional Partnership Funding in application.
Target	Year	2022	> 75% of recipients of DDP Incident Emergency Funding (IEF) and SPF support report that this support contributed positively to the sustainability of their work. > 75% of recipients of DDP IEF and SPF support indicate that DDP interventions effectively responded to threats faced. > 75% of recipients of support from DDP Global and Regional Partner projects indicate an improvement in their security capacities. > 75% of expected success indicators set in DIF accompaniment projects and SPF projects are met.

Output 1.1		DDP provided **Incident Emergency Funding** (monetary contributions) to HRD individuals, organisations or networks under digital threat, in internet repressive environments.	
Output indicator		# of requests received for Incident Emergency Funding. # HRD organisations/networks who received Incidental Emergency Funding. # HRD individuals who received Incidental Emergency Funding. % of recipients of IEF report a qualitative improvement in their security capacities and/or resilience 4 months after receipt of funding.	
Baseline	Year	2020	Qualitative descriptions of risks faced and/or attacks suffered by applicants for IEF.
Annual target	Year 1	2020	200 request received in 2020 for IEF by DDP (for the total basket fund). In 2020 with funding from Denmark, 6 individuals /organisations received incidental emergency funding. > 75% of recipients of IEF report a qualitative improvement in their security capacities and/or resilience 4 months after receipt of funding
Annual target	Year 2	2021	250 request received in 2021 for IEF by DDP (for the total basket fund). In 2021 with funding from Denmark, 6 individuals /organisations received incidental emergency funding. > 75% of recipients of IEF report a qualitative improvement in their security capacities and/or resilience 4 months after receipt of funding
Annual target	Year 3	2022	300 request received in 2022 for IEF by DDP (for the total basket fund). In 2022 with funding from Denmark, 6 individuals /organisations received incidental emergency funding. >75% of recipients of IEF report a qualitative improvement in their security capacities and/or resilience 4 months after receipt of funding.
Output 1.2		DDP **linked/referred HRD individuals**, organisations or networks under digital threat to relevant responders and other stakeholders (Global and Regional Partners, fellows, regional Hivos offices, embassies)	
Output indicator		# HRD organisations/individuals/networks referred for support.	
Baseline	Year	2020	Qualitative descriptions of risks faced and/or attacks suffered by applicants for IEF.
Annual target	Year 1	2020	60 HRD organisations, individuals or networks received critical advice or referral and are able to sustain their work despite digital threats.
Annual target	Year 2	2021	60 HRD organisations, individuals or networks received critical advice or referral and are able to sustain their work despite digital threats.
Annual target	Year 3	2022	60 HRD organisations, individuals or networks received critical advice or referral and are able to sustain their work despite digital threats.
Output 1.3		DDP provided funding and coordination to create **tools and services for HRD individuals,** organisations or networks under digital threat, to use in response to digital emergencies (for example: the Digital First Aid Kit (DFAK))	
Output indicator		# Tools maintained.	
Baseline	Year	2020	Analysis of website visitors.
Annual target	Year 1	2020	Maintain end-user friendly DFAK published online. Support development and maintenance of other learning materials or resources as deemed necessary.
Annual target	Year 2	2021	Maintain end-user friendly DFAK published online. Support development and maintenance of other learning materials or resources as deemed necessary.

Annual target	Year 3	2022	Maintain end-user friendly DFAK published online. Support development and maintenance of other learning materials or resources as deemed necessary.
Outcome 2		HRDs have **access to strengthened global and regional organisations, networks and individuals** providing digital security, protection and digital rights support to civil society.	
Outcome indicator		% of recipients of DDP Global Partnership, Regional Partnership Funding who report that DDP support contributed to their resilience and sustainability. % of Global and Regional Partnerships who successfully collaborate on projects.	
Baseline	Year	2019	Qualitative data included in applications for DDP support. Specific indicators set by responders upon receipt of support by DDP.
Target	Year	2022	> 75% of long-term indicators set by recipients of GPF and RPF are met. > 75% of recipients of GPF and RPF report that DDP support contributed to their resilience and sustainability. At least 2 recipients of GPF and RPF successfully collaborate on projects.
Output 2.1		DDP provided **Sustainable Protection Funding** (monetary contributions) to HRD organisations or networks under digital threat	
Output indicator		# of requests received for Sustainable Protection Funding. # HRD organisations/networks who received Sustainable Protection Funding. % of HRD organisations/networks that report increased capacity to respond to digital threats after receiving Sustainable Protection Funding.	
Baseline	Year	2019	Qualitative assessment of digital threats provided in applications for Sustainable Protection Funding.
Annual target	Year 1	2020	50 request received in 2020 for SPF by DDP (for the total basket fund). In 2020 with funding from Denmark, 3 organisations received sustainable protection funding. > 75% of HRD organisations/networks report increased capacity to respond to digital threats after receiving Sustainable Protection Funding.
Annual target	Year 2	2021	75 request received in 2021 for SPF by DDP (for the total basket fund). In 2021 with funding from Denmark, 3 organisations received sustainable protection funding. > 75% of HRD organisations/networks report increased capacity to respond to digital threats after receiving Sustainable Protection Funding.
Annual target	Year 3	2022	100 request received in 2022 for SPF by DDP (for the total basket fund). In 2022 with funding from Denmark, 3 organisations received sustainable protection funding. > 75% of HRD organisations/networks report increased capacity to respond to digital threats after receiving Sustainable Protection Funding.
Output 2.2		DDP fellows provided **organisational long-term protection to HRD** organisations or networks under digital threat	
Output indicator		# HRD organisations/networks supported in their organisational long term protection by Fellows. # Organisational security focal points within HRD organisations/networks trained by Fellows.	

		% of HRD organisations/networks and organisational focal points that report increased capacity to respond to digital threats after receiving accompaniment through the Digital Integrity Fellowship. Level of satisfaction in accordance with own indicators set at beginning of accompaniment process.	
Baseline	Year	2020	Applications for DIF accompaniment, needs assessments carried out at beginning of accompaniment process.
Annual target	Year 1	2020	With Danish funding; 4 organisations received supported by Fellows in 2020. 8 organisational security focal points were trained by fellows in 2020. > 75% of HRD organisations/networks and organisational focal points report increased capacity to respond to digital threats in completed accompaniment processes. > 75% of organisations report success in specific indicators set by accompanied organisations in collaboration with fellows at beginning of accompaniment process.
Annual target	Year 2	2021	With Danish funding; 4 organisations received supported by Fellows in 2021. 8 organisational security focal points were trained by fellows in 2021. > 75% of HRD organisations/networks and organisational focal points report increased capacity to respond to digital threats in completed accompaniment processes. > 75% of organisations report success in specific indicators set by accompanied organisations in collaboration with fellows at beginning of accompaniment process.
Annual target	Year 3	2022	With Danish funding; 4 organisations received supported by Fellows in 2022. 8 organisational security focal points were trained by fellows in 2022. > 75% of HRD organisations/networks and organisational focal points report increased capacity to respond to digital threats in completed accompaniment processes. > 75% of organisations report success in specific indicators set by accompanied organisations in collaboration with fellows at beginning of accompaniment process.
Output 2.3		DDP provided coordination, financial and logistical assistance to **Digital Integrity Fellows** (monthly stipends, travel stipends, coordinated meetings) to provide long-term holistic protection to HRD organisations or networks under digital threat	
Output indicator		# Digital Integrity Fellows supported with monthly fees and travel stipend. Levels of satisfaction of Fellows with their ability to provide support and the resources provided by DDP. Degree of satisfaction among Fellows with their personal goals as set at the beginning of / renewal of fellowship contract.	
Baseline	Year	2020	Outcome mapping indicators set by Fellows at beginning of / renewal of Fellowship.
Annual target	Year 1	2020	With Danish funding 2 Regional fellows are supported in 2020. > 75% of Fellows report satisfaction with resources, training, intervision and support provided by DDP Fellowship. > 75% of Fellows meet the indicators for personal growth they expect to see in their Fellowship period.

Annual target	Year 2	2021	With Danish funding 2 Regional fellows are supported in 2021. > 75% of Fellows report satisfaction with resources, training, intervision and support provided by DDP Fellowship. > 75% of Fellows meet the indicators for personal growth they expect to see in their Fellowship period.
Annual target	Year 3	2022	With Danish funding 2 Regional fellows are supported in 2022. > 75% of Fellows report satisfaction with resources, training, intervision and support provided by DDP Fellowship. > 75% of Fellows meet the indicators for personal growth they expect to see in their Fellowship period.
Output 2.4		DDP provided **Partnership Funding** to **Global and Regional Partners** who provide **holistic response** to HRD individuals, organisations or networks under digital threat	
Output indicator		# Partners that provide holistic support to HRDs under digital threat who received Global and Regional Partnership Funding from DDP. # HRD organisations/networks who received support via DDP Global and Regional Partners. % of beneficiaries of support from Global and Regional Partners who indicate reduced risk, increased resilience and/or capacity to respond to digital threats.	
Baseline	Year	2020	Assessment of current capacities of Global and Regional partners to be included in the selection criteria of new Partners. Qualitative assessment of risks and vulnerabilities in requests for support to DDP Global and Regional Partners.
Annual target	Year 1	2020	In 2020 with funding from Denmark, 2 Regional organisations received sustainable protection funding. Tbd with the selected partner; amount of HRD organisations/networks who received support via DDP Global and Regional Partners. > 75% of beneficiaries of support from Global and Regional Partners indicate reduced risk, increased resilience and/or capacity to respond to digital threats.
Annual target	Year 2	2021	In 2021 with funding from Denmark, 2 Regional organisations received sustainable protection funding. Tbd with the selected partner; amount of HRD organisations/networks who received support via DDP Global and Regional Partners. > 75% of beneficiaries of support from Global and Regional Partners indicate reduced risk, increased resilience and/or capacity to respond to digital threats.
Annual target	Year 3	2022	In 2022 with funding from Denmark, 2 Regional organisations received sustainable protection funding. Tbd with the selected partner; amount of HRD organisations/networks who received support via DDP Global and Regional Partners. > 75% of beneficiaries of support from Global and Regional Partners indicate reduced risk, increased resilience and/or capacity to respond to digital threats.
Outcome 3		**Accessible, collaborative, resilient and responsive networks of expertise and support** for HRD organisations, individuals or networks under digital threat are developed and strengthened	
Outcome indicator		Reported improved collaboration on emergency support cases among Rapid Responder Network members.	

		% of Field Building participants who indicate their knowledge and capacities improved.	
Baseline	Year	2019	Needs established in applications for support within Rapid Responders Networks. Participative evaluation of collaboration, communication and community.
Target	Year	2022	> 75% of participants of Regional Rapid Responders meetings report that DDP support contributed to their capacities and knowledge. > 75% of participants of Field Building trainings report that DDP support contributed to their capacities and knowledge.
Output 3.1		DDP provided financial and logistical assistance for Rapid Responders Network activities, (regional) meetings and resource creation through **Community Facilitation Funding for strengthened capacity of responders**	
Output indicator		# Collaborative, networking, and co-production meetings organised. % Reported increase of global, regional and local collaboration between emergency responders across organisations.	
Baseline	Year	2020	Participative evaluation of collaboration, communication and community
Annual target	Year 1	2020	Danish funding contributes to 1 regional meeting in 2020. > 75% of Global and Regional Rapid Responder Network activities who report satisfaction with resources and support provided by DDP.
Annual target	Year 2	2021	Danish funding contributes to 1 regional meeting in 2021. > 75% of Global and Regional Rapid Responder Network activities who report satisfaction with resources and support provided by DDP.
Annual target	Year 3	2022	Danish funding contributes to 1 regional meeting in 2022. > 75% of Global and Regional Rapid Responder Network activities who report satisfaction with resources and support provided by DDP.
Output 3.2		DDP facilitated local **holistic safety and security trainings**, **intervision and mentoring** for building capacity of regional trainers and organisational focal points)	
Output indicator		# Of mentors and Trainee Fellows that cooperated in the field-building events (boot-camps, interventions, co-learning and intervision meetings). Increased capacity of Trainee Fellows in technical digital security skills. Increased capacity of Trainee Fellows in facilitation skills. Increased understanding of Trainee Fellows of holistic approach.	
Baseline	Year	2020	Applications to Trainee Fellowships. Monitoring and evaluation of training and boot-camp events. Indicators set in outcome mapping from South-East Asia Pilot 2019.
Annual target	Year 1	2020	Danish funding in 2020 is contributing to 1 Regional holistic training for 14 regional people. > 75% of Trainee Fellows report improved technical digital security skills. > 75% of Trainee Fellows report improved facilitation skills. > 75% of Trainee Fellows report increased understanding of holistic approach.
Annual target	Year 2	2021	Danish funding in 2021 is contributing to 1 Regional holistic training for 14 regional people. > 75% of Trainee Fellows report improved technical digital security skills.

			> 75% of Trainee Fellows report improved facilitation skills. > 75% of Trainee Fellows report increased understanding of holistic approach.
Annual target	Year 3	2022	Danish funding in 2022 is contributing to 1 Regional holistic training for 14 regional people. > 75% of Trainee Fellows report improved technical digital security skills. > 75% of Trainee Fellows report improved facilitation skills. > 75% of Trainee Fellows report increased understanding of holistic approach.
Output 3.3		DDP provided financial and logistical assistance to support **spaces and resources for exchange, dialogue and learning on holistic protection** (for Fellows, HRD organisations, international organisations, funders	
Output indicator		# DDP meetings, network spaces, (online) spaces on holistic methodology facilitated. # Resources created and shared on lessons learned and best practices.	
Baseline	Year	2020	Reports from previous events.
Annual target	Year 1	2020	Danish funding in 2020 contributed to DDP team + fellows meetings, travel to conferences to share best practices, and resources created or contributed to (translations, manuals, copywriting, content creation, designed reports, impact video).
Annual target	Year 2	2021	Danish funding in 2021 contributed to DDP team + fellows meetings, travel to conferences to share best practices, and resources created or contributed to (translations, manuals, copywriting, content creation, designed reports, impact video).
Annual target	Year 3	2022	Danish funding in 2022 contributed to DDP team + fellows meetings, travel to conferences to share best practices, and resources created or contributed to (translations, manuals, copywriting, content creation, designed reports, impact video).

4. Risk Management

Digital Defenders Partnership will continuously monitor existing and potential risks and apply measures to mitigate those risks as can be seen in ANNEX B.

MFA will pay specific attention to potential reputational risks for the MFA and its bilateral relations, that may stem from this project.

5. Inputs/budget

Denmark's contribution for the Digital Defenders Partnership for 2020-2022 is DKK 11,250,000 (eleven million two hundred and fifty thousand).

Detailed budget is attached in Annex A.

6. Management arrangement

The parties will have a dialogue, as appropriate, about the implementation of the activities. DDP will host annual donor meetings to which MFA will be invited.

Digital Defenders Partnership will be fully responsible for managing the activities and its related funds in accordance with the management set-up for Digital Defenders Partnership as directed and approved by the Digital Defenders Partnership Management and oversight bodies. In so doing, Digital Defenders Partnership will consult MFA party regularly on major issues as appropriate.

7. Financial Management

Both parties will strive for full alignment of the Danish support to the implementing partner rules and procedures. The MFA will expect that these are in line with Danida's Financial Management Guidelines.

7.1 Procurement of goods and services

In relation to procurement Stichting HIVOS, Digital Defenders Partnership's procurement rules will apply.

7.2. Transfer of funds

The grant will be disbursed in three instalments based on disbursement requests submitted by Digital Defenders Partnership. The first instalment of DKK 3,750,000 will be disbursed upon the signing of this engagement document. The second instalment of DKK 3,750,000 will be disbursed in January of 2021. The third instalment of DKK 3,750,000 will be disbursed in January 2022.

The grant will be transferred through the below stated bank account.

Account holder:	Stichting HIVOS
Account holder's address:	Grote Marktstraat 47a, 2511 BH The Hague, The Netherlands
Bank:	ABN AMRO (Gustav Mahlerlaan 10, 1082 PP Amsterdam)
Account No.:	839246218
Account name:	Stichting HIVOS
Swift:	ABNANL2A
IBAN:	NL48ABNA0839246218

Digital Defenders Partnership must return a letter or e-mail with acknowledgement of receipt of funds within 14 (fourteen) days after the funds have been received.

Any loss due to the variation of exchange rates between the grant in DKK and the implementing partner's national currency must be covered within the grant.

7.3 Accounting requirements

Accounts shall be kept in accordance with internationally accepted accounting principles and the organisation must follow the basic four-eye principles for all payments.

The total budget cannot be exceeded and shall be used for the agreed purpose only.

The accounts shall at all time be kept updated according to international standards.

The accounts shall be drawn up to the same level of detail as is done in the budget.

7.4 Audit requirements

Denmark’s contribution to the Digital Defenders Partnership must be clearly stated in the organisational financial statements as income and expenditure. This can be in the form of a note together with other donors’ contributions.

The Digital Defenders Partnership must arrange for an annual audit of their accounts to be performed by a certified audit company. The annual audit shall include, but not be limited to inspection of accounting records including examination of supporting documentation of the transactions, confirmation of cash and bank holdings, checking of bank reconciliations, direct confirmation of accounts receivable, an a verification of fixed assets (if applicable).

The MFA has the right to request original, separate and itemised accounts for individual activities including bank statements.

7.5 Financial reporting requirements

The Digital Defenders Partnership will by 30 June each year submit to MFA audited accounts covering the previous financial year in accordance with Stichting HIVOS, Digital Defenders Partnership’s financial management guidelines as approved by Stichting HIVOS’s board.

7.6 Unspent funds

Any unspent balance or any savings of project funds shall be returned to the MFA together with any interest accrued from deposit of Danish funds. In case of jointly financed projects and baskets arrangement where a single bank account is used by multiple development partners interests accrued need not be returned.

7.7 Obligation to report on changes and irregularities

The Digital Defenders Partnership is obliged to inform MFA immediately if any changes, including overspending of budget lines or irregularities in the management of funds are foreseen or have occurred.

8. Monitoring and Evaluation

A project completion report and final audited financial accounts shall be submitted to MFA no later than 30 June 2023.

Annual reports outlining progress based on the results framework, shall be submitted no later than 1 May each year covering the preceding year.

MFA shall have the right to carry out any technical or financial mission that is considered necessary to monitor the implementation of the programme. To facilitate the work of the person or persons instructed to carry out such monitoring missions, the Digital Defenders Partnership shall provide these persons with all relevant assistance, information, and documentation.

After the termination of the programme support MFA reserves the right to carry out evaluation in accordance with this article.

Representatives of the National Audit Office of Denmark shall have the right to:

i) Carry out any audit or inspection considering necessary as regards the use of the Danish funds in question, on the basis of all relevant documentation,

ii) Inspect accounts and records of suppliers and contractors relating to the performance of the contract, and to perform a complete audit

9. Anti-corruption clause

No offer, payment, consideration or benefit of any kind, which could be regarded as an illegal or corrupt practice, shall be made, promised, sought or accepted - neither directly nor indirectly - as an inducement or reward in relation to activities funded under this agreement, incl. tendering, award, or execution of contracts. Any such practise will be grounds for the immediate cancellation of this agreement and for such additional action, civil and/or criminal, as may be appropriate. At the discretion of the Danish MFA, a further consequence of any such practise can be the definite exclusion from any projects funded by the Danish MFA.

10. Child labour clause

The authority, organisation and/or consultant shall abide by the local laws and by applicable international instruments, including the UN Convention on the Rights of the Child and International Labour Organisation conventions.

11. Prevention of sexual exploitation, abuse and harassment

The Digital Defenders Partnership agrees to ensure that the engagement is implemented in an environment free from all forms of harassment, exploitation, abuse and harassment, sexual or otherwise, especially in case of vulnerable groups. Sexual abuse is defined as actual or threatened physical intrusion of a sexual nature, whether by force or under unequal or coercive conditions. Sexual exploitation is defined as any actual or attempted abuse of position of vulnerability, differential power or trust, for sexual purposes, including, but not limited to, profiting monetarily, socially or politically from the sexual exploitation of another. Sexual harassment is defined as any form of unwanted verbal, non-verbal or physical conduct of a sexual nature with the purpose or effect of violating the dignity of a person, in particular when creating an intimidating, hostile, degrading, humiliating or offensive environment.

The above definitions are referred to as Sexual Exploitation, Abuse and Harassment (SEAH).

The Digital Defenders Partnership confirms:
(1) that it has adequate policies/standards or frameworks in place to prevent SEAH[1];
(2) that all employees have been informed about these policies/standards/frameworks; and
(3) that there are appropriate SEAH reporting procedures and complain mechanisms in the organisation including the protection of victims of SEAH and that prompt and adequate action is taken if SEAH is observed, reported or suspected.

In case the development engagement includes subgrantees, the grantee is responsible for ensuring the prevention of SEAH also at the level of subgrantee.

[1] In line/adherence with the Inter Agency Standing Committee's Minimum Operating Standard on prevention of SEA and/or the elements on prevention of SEA of the Core Humanitarian Standard on Quality and Accountability

MFA has zero-tolerance towards SEAH and will consider non-adherence to point 1,2 and 3 as grounds for immediate termination of grant.

12. Suspension

In case of non-compliance with the provisions of this engagement and /or violation of the essential elements mentioned in this engagement the MFA reserves the right to suspend with immediate effect further disbursements to the implementing partners under this engagement.

13. Entry into force, duration and termination

This engagement shall enter into force on the date of signing.

The cooperation between the Parties under this engagement will be for 2020-2022. The duration of the cooperation may be extended by mutual written agreement and within the agreed budget.

Notwithstanding the previous clause each Party may terminate the engagement upon 6 (six) months written notice.

Signatures

On behalf of	On behalf of
Stichting HIVOS	The Ministry of Foreign Affairs of Denmark
Place & date:	
___________________________	__________________________
Signature:	
___________________________	__________________________
Will Janssen	Mette Thygesen
Director Hivos Open Society Programme	Head of Department

Quality Assurance checklist for appraisal of programmes and projects[1]

File number/F2 reference: 2019-27991

Programme/Project name: Support to Digital Defenders Partnership

Programme/Project period: 2020-2022

Budget: DKK 11,250,000

Presentation of quality assurance process:
Two rounds of quality assurance have been conducted by a quality assurance team consisting of a development specialist and a financial management specialist. Meetings have been convened where input/ comments have been provided both verbally and in writing. Feedback from the quality assurance team has been passed on to the partner and reflected in the programme documents. A final screening note by the quality assurance team has been forwarded to the responsible desk officer.

□ The design of the programme/project has been appraised by someone independent who has not been involved in the development of the programme/project.
Comments: The project has been reviewed by a development specialist and a financial management specialist.

□ The recommendations of the appraisal has been reflected upon in the final design of the programme/project.
Comments: Yes.

□ The programme/project complies with Danida policies and Aid Management Guidelines.
Comments: Yes.

□ The programme/project addresses relevant challenges and provides adequate responses.
Comments: Yes.

□ Issues related to HRBA/Gender, Green Growth and Environment have been addressed sufficiently.
Comments: Yes.

□ Comments from the Danida Programme Committee have been addressed (if applicable).
Comments: Not applicable.

[1] This Quality Assurance Checklist should be used by the responsible MFA unit to document the quality assurance process of appropriations where TQS is not involved. The checklist does not replace an appraisal, but aims to help the responsible MFA unit ensure that key questions regarding the quality of the programme/project are asked and that the answers to these questions are properly documented and communicated to the approving authority.

□ The programme/project outcome(s) are found to be sustainable and is in line with the partner's development policies and strategies. Implementation modalities are well described and justified.
Comments: Yes. The project is closely aligned with the partner's strategies and draws on the partners overall results framework.

□ The results framework, indicators and monitoring framework of the programme/project provide an adequate basis for monitoring results and outcome.
Comments: Denmark is providing earmarked funds for Digital Defenders Partnership (DDP). The results framework, indicators and monitoring framework are based on and closely aligned to DDP's overall frameworks. Efforts to ensure donor harmonization makes it more difficult to demand specific and different frameworks for the Danish grants. Monitoring will also happen through donor meetings and coordination as well as continuous dialogue with the partner.

□ The programme/project is found sound budget-wise.
Comments: Yes.

□ The programme/project is found realistic in its time-schedule.
Comments: Yes.

□ Other donors involved in the same programme/project have been consulted, and possible harmonised common procedures for funding and monitoring have been explored.
Comments: MFA have participated as observer in a donor meeting prior to the signing of the contract.

□ Key programme/project stakeholders have been identified, the choice of partner has been justified and criteria for selection have been documented.
Comments: The partner has been selected based on its central position in the landscape of organisations working with digital resilience of civil society organisations.

□ The executing partner(s) is/are found to have the capacity to properly manage, implement and report on the funds for the programme/project and lines of management responsibility are clear.
Comments: Yes.

□ Risks involved have been considered and risk management integrated in the programme/project document.
Comments: Yes, cf. Annex B.

□ In conclusion, the programme/project can be recommended for approval: yes

Date and signature of desk officer: 8 June 2020 ________________

Date and signature of management 5 June 2020