**ROLE PROFILE**

| | | | |
|---|---|---|---|
| **JOB TITLE:** | Digital Protection Coordinator for Eastern Europe and Central Asia (EECA) | **REPORTING TO:** | Digital Protection Manager/ Head of Digital Protection |
| **TEAM:** | Digital Protection | **DATE:** | July 2026 |
| **LOCATION:** | Remote (based in EECA region) | **CONTRACT TYPE:** | Full time, Permanent |
| **WEEKLY HOURS:** | 35 hours | **SALARY:** | Grade G (€36,241 - €66,700) |

## Principal Objective of the Role:

**Role Purpose:**

Front Line Defenders (FLD) is working to expand its capacity to support Human Rights Defenders (HRDs) and Human Rights Organisations (HROs) in managing risks associated with the use of digital information and communications. We offer direct on the ground support to HRDs/HROs with the help of a team of Digital Protection Coordinators and Consultants (DPC). FLD is headquartered in Ireland but we are seeking to hire a candidate for a staff role who is based in the EECA region, to deliver direct digital protection support to HRDs/HROs at risk.

## Responsibilities:

The key accountability and associated duties include:

**1 Support HRDs/HROs**

**Provide direct, effective, timely (when possible) in-person one-to-one and group digital protection support to selected HRDs/HROs.**

- Actively research on digital protection situation of HRDs/HROs in the region. Evaluate the situation of risk, changes and new trends.
- Propose HRDs/HROs at risk for our support. Assist relevant regional Protection Coordinator in prioritisation of those HRDs/HROs who are most at risk and in deciding who we would deliver support to.
- Analyse and assess the specific digital protection risks, vulnerabilities and capacities of the HRDs/HROs receiving or due to receive support. Collect data from multiple sources to inform support and training needs to understand HRDs/HROs digital protection weaknesses, missing and valuable resources, map the information, communication, devices, services/servers used landscape.
- Use above information to structure, in interactive cooperation with specific HRDs/HROs

a support or training curriculum for constantly changing contexts, risks, and needs. Draft specific support plan or training content. Liaise with FLD colleagues to support the development of plans and curricula to meet bespoke HRDs/HROs needs.

- Provide direct, effective, timely (when possible) in-person one-to-one and group digital protection support to selected HRDs/HROs. Promote and coordinate the delivery of support. Organise and deliver support process starting with awareness raising of risks and potential mitigation, coming up with a plan to implement solutions with HRD/HRO and help carry out this plan which includes training, workshops, meetings, sessions to help facilitate learning, advice on acquiring specific hardware or services and direct support practical implementation of solutions that include learning, changing habits and the installation, configuration and use of tools in daily work.
- Help find local trainers and champions to assist in delivery of the support and the continuation of the process and maximise its effectiveness.
- Help create and maintain an up to date library of written guides for human rights defenders as learning material and to highlight risks and how best to mitigate them. Assist in creating materials for Security in-a-Box and other guides.
- Follow up each engagement after a certain period of time (4-6 weeks) to understand how the implementation of solutions is going and to help further in the sustainability of the approach used.
- Mentor local champions and trainers so they can continue supporting HRDs/HROs at risk and in need.
- Engage directly with HRDs to clarify misunderstandings they may have about digital protection, walking them through various processes, providing a listening ear and seeking to reduce their stress through provision of expert advice

2 **Regional Knowledge, Awareness & Assessment:**
**As this role is an expert, specialist role, it is critical that a relevant regional technical knowledge and awareness is maintained to provide the best class of digital protection available to HRD's and support assessment of needs.**

- Maintain an up to date knowledge base including awareness of new digital protection technologies and updates to old ones. Frequently research information security topics to maintain awareness as it evolves and highlight relevant issues that are emerging. Understanding new risks, solutions and recommendations specific to regional digital protection needs.
- Continually evaluate and upskill on the risks associated with the usage of common internet services, software, tools, devices.
- Take time to understand the context (regional, identity related, work related), environment and specific vulnerabilities of people using these tools. Use this knowledge to inform day to day actions and advice.
- Maintain focused attention on the technical aspects of the work to ensure a high quality of delivery.
- Review, evaluate and update risk assessment techniques and how we use them to understand risks of HRDs/HROs one is working with.
- Understanding the impact on the digital protection support we give and come up with new ways to help in the general context of the region regarding upcoming and current legal frameworks, digital harassment and intimidation patterns and specific surveillance

and control equipment governments in the region are promoting or acquiring.

**3 Collaboration**

**Liaise with relevant colleagues internally to provide mutual support to each other in the course of delivery of your work.**

- Collaborate with colleagues as appropriate such as Protection Coordinators on different issues. This shared approach to supporting HRD's at risk supports a better delivery of service to those we support. Maintain accurate notes of such activities, discussions and agreements and keep your colleagues updated as situations progress.
- Work in collaboration with the protection and visibility teams to support them in their external advocacy work. This is one of the components of FLD's holistic protection approach.
- Support colleagues in the grants teams in their assessment of whether the suggested approach is a correct mitigation strategy to help the HRD/HRO.
- Appropriately follow-up with HRDs/HROs to ensure that needed digital protection support is delivered, we avail of opportunities to take proactive measures and record and embed any learning.
- Take part in relevant internal FLD meetings (remote and in-person) to better facilitate the holistic/integrated support to HRDs/HROs.

**4 Partnerships & Networking**

**Identify and develop relationships with key contacts to support the optimum delivery of digital protection support to HRD's.**

- Develop and foster relationships with other organisations doing similar work to understand gaps in our capabilities and how those gaps can be filled by using external support
- Coordinate with partners on a needs basis to provide support to mitigate risks that we may not be able to address in-house
- Maintain frequent contact with organisations and people in the region of focus who can share information to keep you up to date on the context as it evolves.
- Represent FLD in the region in relation to digital protection.
- Participate as FLD's DPC in digital protection national and international events.

**5 Impact Assessment & Reporting**

**Use multiple data sources to capture feedback and assess the impact that FLD's supports are making to HRD's at risk, reporting these learning internally to aid organisational development.**

- Submit written monthly reports documenting work.
- Collect frequent anecdotal feedback from HRDs at risk to record how they have engaged with the support provided capturing what tangible increase in their digital awareness, safety and behaviour they have perceived.
- Design, administer, analyse and report on qualitative questionnaires to HRDs for evaluation on the above.
- Design, administer, analyse and report on evaluation of training supports delivered using different ways of gathering information.

- Report on any chain-reaction effects being observed and reported among the those receiving support i.e. those who receive the support sharing with their peers
- Collate and share data for the purpose of internal reporting on coordination and collaborations on work done with HRDs through various formats. This includes monthly year end reporting.

*This job description is intended as a summary of the primary responsibilities of and qualifications for this role. The job description is not intended as inclusive of all duties an individual in this position might be asked to perform based on requirements either now or in the future.*

| **Reporting Structure:** | |
|---|---|
| Directly: Nil | Indirectly: Nil |
| **Key Relationships:** | |
| Internal: Digital Protection Coordinators, Protection Coordinators, Communication team, Visibility team, Capacity Building team, Grants team, and other teams depending on tasks and team coordination requirements | External: Human Rights Defenders (HRDs), Human Rights Organizations (HROs), Partners, network contacts |

## Salary

The salary range for this role is €36,241 - €66,700, aligned with Grade G on the pay scale.

The role holder is responsible for complying with relevant tax and other legal requirements in their country of residence.

Benefits include 26 days annual leave, Pension, Health Insurance, Income Protection, Life Assurance, Employee Assistance Scheme (EAP), Monthly Well-Being Provisions, Laptop, Mobile Phone.

## Person Specification

**Knowledge and Skills:**

Essential:

- Prior experience in working with HRDs/HROs in the EECA region.
- Demonstrable and verifiable experience in providing digital security support (technical and conceptual) to HRDs/HROs in EECA in general;
- Interest and aptitude in information technology.
- Understanding administration of different operating systems for both computers and phones.
- Understanding of securing computers, phones and networking on the level of computer and network administrators.
- Very good ICT skills, on the level of computer and network administrators -understanding

technical concepts and also practical hands-on knowledge of how to manage devices, programs and services;

- Demonstrable and verifiable skills in device administration covering different computer and mobile operating systems; experience in computer and device security configurations is a required skill;
- Understanding of online services including email and social media platforms.
- Understanding of information and communication technology risks.
- Strong understanding of the human rights context in the region of work and prior good experience in working with HRDs/HROs in the region.
- Resourcefulness to be able to respond in cases of emergencies
- Ability to formulate and conduct training and other learning processes in an accessible manner.
- Demonstrable and verifiable experience in conducting digital protection support and trainings for HRDs/HROs, from needs and risk assessment, agenda development and evaluation;
- Proven ability to train and coach adults in digital security.
- Ability to simplify complex technical terminologies into simple human understandable terms.
- Ability to work independently the majority of the time.
- Fluency in English and Russian, and working knowledge of one of the EECA regional languages such as Kazakh, Georgian, Ukrainian, Kyrgyz, Armenian, Tajik, Uzbek, or Belarusian
- Must be based in EECA, and be able to travel within the region;
- Previous good experience with individual, group and organisations digital protection support and training.

Desirable:

- Understanding of the specific risks faced by and protection need of LGBTIQ+, women HRDs and feminists in the region
- Experience of holistic protection
- Good interpersonal skills allowing them to interact with HRDs at risk in situation of stress
- Knowledge of the other languages used in the region

**Experience:**

Essential:

- Minimum 3 years experience in digital protection support.
- Minimum 1 year of experience of working with HRD/HRO in the respective region.
- Provided digital protection support and training for individual, group and organisations.
- IT problem solving in all major operating system (Windows, Mac, Android and iOS).
- Participation in national and international IT conferences.

Desirable:

- Active and trusted member of the human rights community.
- IT systems administrator, IT support experience.
- Creating websites and programming.
- Servers administration experience.
- Linux operating systems administration experience.
- Holistic security in context of digital protection experience, support, training, etc.

**Other requirements:**

- Be based in the region DPC work in
- Be able to travel in the region

**Front Line Defenders Values:**

**1. Working With Colleagues:**

- Respect for the Individual
- Building Trust
- Collaborative Working
- Communication With Each Other

**2. Developing Myself:**

- Self-Awareness
- Adapting to Change
- Proactive Learning
- Managing My Well-being

**3. Leadership:**

- Strategic Thinking
- Engaging With People
- Stewardship of Resources

**Selection and Appointment:**

- To apply, candidates need to submit a copy of their application - CV and cover letter - via the 'Apply Now' button
- Cover letters should be addressed to **Head of Digital Protection**
- Only shortlisted candidates will be invited to attend for interview;
- It is anticipated interviews will be held in end of July 2026.
- The appointment is expected to be effective from August 2026.
- **Closing date; 4pm** (local Irish time) on **01 July 2026**

**Frontline Defenders is an Equal Opportunities Employer**