

EUROPEAN EXTERNAL ACTION SERVICE



Annex 1

<p align="center">European Union Mission in Armenia EUM Armenia 1-2025 Call for Contributions for the Civilian CSDP Young Professional Experts Pilot Programme Requirements and Job Descriptions</p>				
Organisation:	European Union Mission in Armenia			
Job location:	As indicated below			
Employment regime:	As indicated below			
Job titles/ vacancy notice:	Ref.:	Name of the post:	Location:	Availability:
	<u>Seconded (3)</u>			
	ARM YPE 01*	Press and Public Information Officer (YPE)	Yeghegnadzor	ASAP
	ARM YPE 02*	Cyber Security Officer (YPE)	Yeghegnadzor	ASAP
	ARM YPE 03*	Mission Analytical Capability (MAC) Analyst (YPE)	Yeghegnadzor	ASAP
Deadline for applications:	Monday, 16 June 2025, at 17:00 (Brussels time)			
Applications must be submitted to:	<p>1) You have the nationality of an EU Member State: you must use Goalkeeper to apply:</p> <p>a) You are already registered on Goalkeeper AND you have an EU Login: https://goalkeeper.eeas.europa.eu/registrar/web</p> <p>b) You do not have a Goalkeeper account or an EU Login: https://goalkeeper.eeas.europa.eu/registrar/web/DPA/357/details.do</p> <p><i>Please note: Seconded positions are only available for candidates already validated in the database of their Seconding Authority. Please contact your National Seconding Authority for more information on applying for vacant seconded positions. We cannot provide contact details of National Seconding Authorities.</i></p>			
Information:	For more information relating to selection and recruitment, please contact			

	<p>the Civilian Operations Headquarters (CivOpsHQ):</p> <p>Ms Tanja HERTOGHE</p> <p>CIVOPSHQ-HR-EUM-ARMENIA@eeas.europa.eu</p> <p>+32 (0)2 584 21 91</p>
--	---

*Availability of post is subject to Deployment Plan approval.

Low and/or Medium Risk Non-Family Mission

The European Union Mission in Armenia bears a Low and Medium Risk Non-Family Mission status. As such, the Mission takes no responsibility for family members of mission members visiting or habitually residing in the country. Only international mission members are covered by the Mission status (SOMA), MEDEVAC or security/evacuation arrangements and use of Mission assets including vehicles. All costs for family members in the Mission area, including insurance, are the respective staff member responsibility. Subject to deterioration of the security situation and possible evolution of the SIAC risk rating, the Head of Mission will propose, in consultation with the EEAS Security Department, to the Civilian Operation Commander, to take measures to change the application of the Low and/or Medium Risk Non-Family status into High Risk Non-Family status.

Seconded personnel – For seconded positions, only personnel nominations received through official channels from EU Member States will be considered. EU Member States will bear all personnel-related costs for seconded personnel, including salaries, medical coverage, travel expenses to and from the Mission area (including home leave) and allowances other than those paid according to the Council documents 7291/09 (10 March 2009) and 9084/13 (30 April 2013).

Tour of duty – Subject to the adoption of the Council Decision extending the Mission mandate and approving the appropriate Budgetary Impact Statement, the duration of the deployment should be of 12 months, renewable for a second year.

Admission to the Young Professional Expert Programme shall not entitle the successful candidates to a future employment or give priority to be recruited for any of the positions in the civilian CSDP missions. Applications under the contracted regime will not be considered for a one-year period after completion of the programme.

The Civilian Operations Commander requests that EU Member States propose candidates for the for EUM Armenia, according to the requirements and profiles described below:

I. GENERAL CONDITIONS

Citizenship – Candidates must have a citizenship of an EU Member State.

Age – Candidates must be at least 18 years and maximum 32 years old at the deadline for application.

Integrity – Candidates must maintain the highest standards of personal integrity, impartiality and self-discipline within the Mission. Selected candidates are not allowed to provide or discuss any information or document as a result of access to classified and/or sensitive information relating to the Mission or respective tasks and activities. They shall carry out their duties and act in the interest of the Mission.

Flexibility and adaptability – Candidates must be able to work in arduous conditions with a limited network of support, with unpredictable working hours and a considerable workload. They must have the ability to work professionally as a member of a team, in task forces and working groups with mixed composition (e.g. civilian and military staff) and be able to cope with extended separation from family and usual environment.

Availability – Candidates must be able to undertake any other tasks related with the competencies, responsibilities and functions of the respective position within the Mission, as required by the Head of Mission.

Serious deficiencies in any of these general conditions may result in repatriation/termination of the secondment/contract.

II. REQUIREMENTS

II.A Essential requirements

The following are essential requirements in respect of civilian international experts to the Missions for all Job Descriptions:

Physical and mental health – Candidates must be physically fit and in good health without any physical or mental problems or substance dependency which may impair operational performance in the Mission and in its Area of Operation. Selected candidates should undergo an extensive medical examination as requested by the seconding authority or the Mission in accordance with “Fit to work clearance” procedure prior to recruitment/deployment to prove that they comply with the requirement.

Education and training – Candidates should have a recognised qualification under the European Qualifications Framework (EQF), or equivalent, at a level specified in the individual job descriptions. Candidates are advised to verify their compliance through the link: <https://ec.europa.eu/ploteus/content/descriptors-page>.

Professional experience - A minimum of two years of professional experience, gained after reaching the age of 18 and having fulfilled the education requirements (including acquired through relevant internships, i.e. EULEX Kosovo Internship Programme) is required to apply for this programme. Applicants should not have previously participated in any civilian CSDP Mission.

Knowledge – Candidates should have knowledge of the EU Institutions and Mission Mandate, particularly related to the Common Foreign and Security Policy (CFSP), including the Common Security and Defence Policy (CSDP).

Skills and abilities

Language skills – Candidates must have the understanding, speaking, and writing proficiency in the working languages of the Mission. Certain positions may require higher language skills further specified in the individual job descriptions. The Mission may seek to facilitate language training and where appropriate, specialist language training, for newly recruited mission staff members. Candidates are advised to verify their proficiency through the following link: <https://europa.eu/europass/en/common-european-framework-reference>.

Communication and interpersonal skills – Candidates must have excellent interpersonal and communication skills, both written and oral.

Organisational skills – Candidates must have excellent organisational skills, with the ability to prioritise work to meet deadlines, and a concern for order and accuracy.

Digital skills – Candidates must have basic digital skills in the competency areas: information and data literacy, communication and collaboration, digital content creation, safety and problem solving. Candidates are advised to verify their proficiency through the following link: <https://digital-strategy.ec.europa.eu/en/news/test-your-digital-skills-and-thrive-digital-world>.

Driving skills – Candidates must be in possession of a valid – including Mission area – civilian driving licence for motor vehicles (Category B or equivalent). They also must be able to drive any 4-wheel-drive vehicle.

Serious deficiencies in any of these general conditions may result in repatriation/termination of the secondment/contract.

II.B Desirable requirements

Knowledge of the Mission area – Candidates should have a good knowledge of the history, culture, social and political situation of the region and also knowledge of the police, judiciary and governmental structures, as applicable.

Knowledge and experience of Security Sector Reform – Candidates must be acquainted with Security Sector Reform concepts and practices, especially in the Mission area, as applicable.

Training and experience – Candidates should have attended a Civilian Crisis Management Course or equivalent.

Language – Knowledge of local language(s), depending on the job tasks and responsibilities.

Driving licence – Category C driving licence.

III. ESSENTIAL DOCUMENTS AND EQUIPMENT FOR SELECTED CANDIDATES

Passport – Selected candidates must have a biometric passport from their respective national authorities valid for at least six months. If possible, a Service Passport or Diplomatic Passport should be issued.

Visas – Contributing States and selected candidates must ensure that visas are obtained for entry into the Mission area prior to departure from their home country. It is also essential to obtain any transit visas, which may be required for passage through countries on route to the Mission.

Required Personnel Security Clearance (PSC) or Certificate of Good Conduct – Selected candidates will have to be in possession of the necessary level of a Personnel Security Clearance (PSC) as specified in the respective job descriptions. In case of lack of such requirement in the job description, selected candidates are required to present a valid official document from their respective country's competent National Authority confirming the lack of convictions for crimes or offences under common law, not older than 3 months (the so-called **Certificate of Good Conduct**).

In case of the PSC requirement: seconded Young Professional Experts must provide the original certificate of the national security clearance or a proof of the initiation of the process upon deployment.

In any case, the final PSC certificate must be presented within 12 months from the deployment. Failing to meet this requirement will result in the termination of the secondment and no extension can be granted.

In case of the **Certificate of Good Conduct**, seconded experts must deliver such a certificate to their respective Seconding Authority. In case of possession of multiple nationalities, or if a candidate has or had his/her residence in a country, which is not his/her country of origin, a certificate must be issued by every country where the selected candidate has had his/her residence for a period longer than 1 year during the last 5 years preceding the deployment (except if he/she resided there prior to reaching the age of 18 years).

Certificate/booklet of vaccination – Selected candidates must be in possession of a valid certificate/booklet of vaccination showing all vaccinations and immunisations received. They also must be vaccinated according to the required immunisations for the Area of Operation of the Mission.

Medical certificate – Selected candidates should undergo an extensive medical examination and be certified medically fit for Mission duty. A dental examination is also required to certify that no eminent dental issues are foreseen.

For seconded selected candidate, the fitness to work certificate must be sent to the Medical Adviser of the Mission before joining the Mission. Medical data will be handled with confidentiality and in line with EU Charter of Fundamental Rights and the Standard Operating Procedure on the protection of personal data (CivOpsCdr Instruction 12-2018 as amended.)

The Heads of Mission reserve the right to reject the recruitment of any selected candidate that proves to be medically unfit to work in a civilian CSDP Mission.

Personal protection equipment – It is recommended that national authorities provide seconded selected candidates with protection equipment.

Deficiencies in any of the documents requested for a specific position may result in failure of the selection process.

IV. ADDITIONAL INFORMATION

Equal opportunities – The EEAS is committed to an equal opportunities policy for all its employees and applicants for employment. As an employer, the EEAS is committed to promoting gender equality and to preventing discrimination on any grounds. It actively welcomes applications from all qualified candidates from diverse backgrounds and from the broadest possible geographical basis amongst the EU Member States. It aims at a service, which is truly representative of society, where each staff member feels respected, is able to give their best and can develop their full potential.

Gender balance – The EU strives for improved gender balance in CSDP operations in compliance with EU policy and UNSCR 1325 on Women, Peace and Security (WPS). The CivOpsHQ encourages the EU Member States and European Institutions to take this into account when putting forward candidates at all levels.

Applications – Applications will be considered only when using the online application form (AF) accessible on the Goalkeeper-Registrar software module, indicating which position(s) the candidate is applying for.

In relation to the Concept Note on Civilian CSDP Young Professional Expert Pilot Programme (EEAS(2024)1538), Young Professional Experts must be at least 18 years and maximum 32 years old at the deadline for applications; they furthermore must have not previously participated in any civilian CSDP Mission.

Selection process – Candidates considered to be most suitable will be shortlisted and, if needed, interviewed in Brussels, at the Headquarters of the Mission or by video conference before the final selection is made. If seconded candidates are required to travel to Brussels/Mission Headquarters for interviews, the Contributing States will bear any related costs. Candidates should be selected on the basis of relevant competence and experience, while strict priority shall be given to seconded candidates.

Information on the outcome – Contributing States will be informed about the outcome of the selection process after its completion.

Training – The selected candidates should complete Missionwise and e-SAFE modules, which are designed for the delegations or an equivalent course. The modules can be accessed in the following link: <https://webgate.ec.europa.eu/eeas/security-e-learnings>.

Pre-Deployment Training (PDT) – The selected candidates should have undergone Pre-Deployment Training in accordance with the CSDP agreed Training Policy, or a national alternative of the course.

Data protection – The EEAS, and its Department CivOpsHQ, processes personal data pursuant to Regulation (EC) 2018/1725 on the protection of individuals with regard to the processing of personal data by the EU institutions, bodies, offices and agencies and on the free movement of such data. The Privacy Statement is available on the EEAS website.

V. JOB DESCRIPTIONS

The current reporting lines of the following job descriptions might be subject to modification based on operational requirements and in line with the principles set out in the Operational Plan (OPLAN).

SECONDED POSITIONS

Position Name: Press and Public Information Officer (YPE)	Employment Regime: Seconded	
Ref. Number: ARM YPE 01*	Location: Yeghegnadzor	Availability: ASAP
Component/Department/Unit: Chief of Staff Office/ Press and Public Information	Security Clearance Level: N/A	Open to Contributing Third States: NO

1. Reporting Line

The Press and Public Information Officer (YPE) reports to the Head of Press and Public Information.

2. Main Tasks and Responsibilities:

- To facilitate and assist the Press and Public Information Office in creating and promoting a positive and transparent public image of EUMA through various channels and outreach activities;
- To contribute to the design and execution of outreach activities and public information campaigns for the Mission;
- To disseminate internal information and materials to Mission members;
- To assist in preparation of press conferences and media events;
- To assist in developing and maintaining the EUMA website and social media channels.

3. General Tasks and Responsibilities:

- To identify and report on lessons learned and best practices within the respective area of responsibility;
- To contribute and ensure timely reporting on activities within the respective area of responsibility;
- To take account of gender equality and human rights aspects in the execution of tasks;
- To undertake any other related tasks as requested by the Line Manager(s).

4. Essential Qualifications and Experience:

- Successful completion of university studies of at least 3 years attested by a diploma **OR** a qualification in the National Qualifications Framework which is equivalent to level 6 in the European Qualifications Framework **OR** a qualification of the first cycle under the framework of qualifications of the European Higher Education Area, e.g. Bachelor's Degree. The qualification should be in any of the fields of Communications, Political studies, International Relations, Humanities, Social sciences or other related field;
AND
- After having fulfilled the education requirements, a minimum of 2 years of relevant professional experience.

5. Essential Knowledge, Skills and Abilities:

- Experience and skills in digital communication (website management, managing social media accounts, visual communication);
- Drafting and presentation skills;
- English language skills: minimum B2 (Independent User).

6. Desirable Qualifications and Experience:

- Experience in the field of institutional communication;
- Proficiency with social media and graphic design software;
- International experience, particularly in crisis areas with multinational and international organisations.

7. Desirable Knowledge, Skills and Abilities:

- Local press and media environment awareness;
- Experience in multimedia content production
- Knowledge of Russian and/or Armenian language(s).

Position Name: Cyber Security Officer (YPE)	Employment Regime: Seconded	
Ref. Number: ARM YPE 02*	Location: Yeghegnadzor	Availability: ASAP
Component/Department/Unit: Mission Support/CIS	Security Clearance Level: EU CONFIDENTIAL	Open to Contributing Third States: NO

1. Reporting Line

The Cyber Security Officer (YPE) reports to the Cyber Security Officer.

2. Main Tasks and Responsibilities:

- To facilitate and to assist the Cyber Security Officer in the implementation of Mission's cyber security controls;
- To assist to the Communication and Information Systems first-level support, initial troubleshooting for all directly reported issues and tickets assigned by the Help Desk and quickly restore the affected services;
- To administer and troubleshoot cloud, system, and network security solutions, updating software with latest security patches and ensuring the proper defences are present for each network and system resource;
- To identify, assess, and propose penetration tests and/or vulnerability assessment solutions and tools;
- To assist to the security systems configuration, analyse security requirements and recommend improvements;
- To monitor network traffic for suspicious behaviour, IT security metrics, SIEM and security logs, systems and service performance and security posture, providing periodic status reports;
- To research, evaluate, recommend, and introduce new IT security tools, techniques, services, and technologies to improve and innovate the Mission's IT security solutions portfolio;
- To support development and participate in the Mission's Cybersecurity Incident Response Team and work closely with stakeholders involved with Cybersecurity issues;
- To conduct regular technical IT security risk and control assessments/audits of systems and infrastructure, and provide actionable dashboards and data regarding status of remediation of security findings to vulnerability owners;
- To maintain the use of security tools (i.e. firewalls, data encryption, security certificates, IDS, IPS, SIEM) and services, to protect the Mission's data, electronic information, systems, and infrastructure.

3. General Tasks and Responsibilities:

- To identify and report on lessons learned and best practices within the respective area of responsibility;
- To contribute and ensure timely reporting on activities within the respective area of responsibility;
- To take account of gender equality and human rights aspects in the execution of tasks;
- To undertake any other related tasks as requested by the Line Manager(s);
- To support the appointed PoC for Cyber matters liaising with the CivOpsHQ.

4. Essential Qualifications and Experience:

- Successful completion of university studies of at least 3 years attested by a diploma in Computer Science, Information Systems or equivalent education OR a qualification in the National Qualifications Framework which is equivalent to level 6 in the European Qualifications Framework in Computer Science, Information Systems or equivalent education OR a qualification of the second cycle under the framework of qualifications of the European Higher Education Area, e.g. Bachelor's Degree;
AND

- After having fulfilled the education requirements, a minimum of 2 years of relevant professional experience.

5. Essential Knowledge, Skills and Abilities:

- Knowledge of industry best practices in network, application, hardware and OS platform security and global security standards;
- Problem solving skills and the ability to understand and analyse complex technical end-users' problems and requests, and successfully manage and solve them daily;
- Ability to develop awareness campaigns;
- Ability to advise on security and counter intelligence;
- English language skills: minimum B2 (Independent User).

6. Desirable Qualifications and Experience:

- To possess current/valid professional industry certification(s), any one or more of CISSP, CISM, CISA, CRISC OR a combination of postgraduate certificates and certifications such as CompTIA Security+, CEH Certified Ethical Hacker, or GIAC certifications in cyber security or information security;
- Experience with Microsoft Windows/Linux server, Microsoft Active Directory and Group Policies, Microsoft 365 Security platform (i.e. Defender ATP), network routers and switches, next generation firewalls, data and drive encryption tools, and CA/PKI solutions;
- Professional experience in managing IT security and hands-on experience with related technologies, i.e. Firewalls, SIEM, IDS/IPS, NAC, MFA, Endpoint Security, and security hardening of networks, systems, and services;
- A combination of professional and relevant expertise and/or certifications in Microsoft, Cisco, Palo Alto, Vmware, EMC products and technologies;
- Familiarity with one or multiple ISO/IEC 27001, 27002 and 27005 Standards to help establishing a formal IT security governance and framework of operations, while also supporting in the system auditing processes;
- Background and familiarity with IT infrastructure methodologies, processes, and practices (i.e. ITSM/ ITIL);
- Experience with and/or good knowledge of modern security tools and products, including vulnerability scanners, analytical and testing tools (i.e. SPLUNK, MISP, Snort, Nessus, or similar);
- International experience, particularly in crisis areas with multi-national and international organisations.

7. Desirable Knowledge, Skills and Abilities:

- Knowledge of EU information security standards and formal accreditation processes;
- Knowledge of information system risks methodologies, cybersecurity frameworks (e.g. NIST or ISO 27000) and have good understanding of incidents investigation steps and processes;
- Project management skills and, possibly, practical experience with project management tools;
- Problem solving attitude and analytical ability to analyse complex IT systems configuration;
- Knowledge of information technology and security issues;
- Ability to develop and audit security systems using traceability framework;
- Knowledge of Russian and/or Armenian language(s).

Position Name: Mission Analytical Capability (MAC) Analyst (YPE)	Employment Regime: Seconded	
Ref. Number: ARM YPE 03*	Location: Yeghegnadzor	Availability: ASAP
Component/Department/Unit: Chief of Staff Office	Security Clearance Level: EU CONFIDENTIAL	Open to Contributing Third States: NO

1. Reporting Line

The Mission Analytical Capability (MAC) Analyst (YPE) reports to the Chief of Staff.

2. Main Tasks and Responsibilities:

- To facilitate and assist the Mission Analytical Capability (MAC) Analyst in creating and promoting the Mission situational awareness in accordance with the agreed Mission Analytical Capability (MAC) concept;
- To contribute to the establishment, where required and as directed by the Mission Analytical Capability (MAC) Analyst, liaison arrangements with relevant counterparts;
- To provide input and draft Mission reports, including special reports;
- To disseminate internal information and materials to Mission members;
- To help if so directed with analysis related to hybrid threats including disinformation and/or other theatre-specific emerging challenges;
- To identify the specific dynamics and actors linked to the situation of the Area of Operation;
- To identify, monitor and report on emerging and on-going hybrid and other threats/challenges in the area of operation and against the Mission, the host nation and EU interests, and to further develop the Missions' 'early warning' capacity on hybrid and other threats, in coordination with relevant actors in the Mission;
- To manage Mission interaction with EU Intelligence and Situation Centre (INTCEN)/Single Intelligence Analysis Capacity including the Hybrid Fusion Cell.

3. General Tasks and Responsibilities:

- To identify and report on lessons learned and best practices within the respective area of responsibility;
- To contribute and ensure timely reporting on activities within the respective area of responsibility;
- To take account of gender equality and human rights aspects in the execution of tasks;
- To undertake any other related tasks as requested by the Line Manager(s).

4. Essential Qualifications and Experience:

- Successful completion of university studies of at least 3 years attested by a diploma **OR** a qualification in the National Qualifications Framework which is equivalent to level 6 in the European Qualifications Framework **OR** a qualification of the first cycle under the framework of qualifications of the European Higher Education Area, e.g. Bachelor's Degree;
AND
- After having fulfilled the education requirements, a minimum of 2 years of relevant professional experience.

5. Essential Knowledge, Skills and Abilities:

- Analytical skills and knowledge of information collection;
- Writing and reporting skills;
- English language skills: minimum B2 (Independent User).

6. Desirable Qualifications and Experience:

- Experience in use of analytical IT packages and processes;

- Successful completion open-source intelligence courses;
- Experience in analysing hybrid threats and other emerging threats;
- International experience, particularly in crisis areas with multi-national and international organisations.

7. Desirable Knowledge, Skills and Abilities:

- Knowledge of Russian and/or Armenian language(s).