www.coe.int/cybercrime

CALL FOR EXPRESSION OF INTEREST
for SHORT-TERM CONSULTANTS
on an AD-HOC BASIS

Organisation:	Council of Europe Cybercrime Division, DG1 Cybercrime Programme Office of the Council of Europe (C-PROC), Bucharest, Romania
Object:	Consultancy services on cybercrime and electronic evidence
Required expertise:	Expertise on cybercrime and electronic evidence: 1. Legislation on cybercrime and related issues (child protection, data protection, terrorist use of information technology, money laundering, telecommunication regulations); 2. Cybercrime and cybersecurity policies and strategies and inter-agency cooperation; 3. Strengthening of specialized cybercrime units; 4. Law enforcement training on cybercrime and electronic evidence; 5. Judicial training on cybercrime and electronic evidence; 6. Financial investigations and prevention of online fraud and money laundering; 7. Public/private cooperation, cybercrime prevention and cybercrime reporting systems; 8. International cooperation.
Notice issued:	02 December 2019
Deadline for applications:	31 January 2020

BACKGROUND INFORMATION AND SCOPE OF THE CALL

The Cybercrime Division of the Council of Europe – through its Cybercrime Programme Office (C-PROC) in Bucharest, Romania – is implementing a range of capacity building projects on cybercrime and electronic evidence worldwide.

Current projects include (for more information, click on the respective Project):

- GLACY+ project on Global Action on Cybercrime Extended
- CyberCrime@Octopus
- CyberEast - Action on Cybercrime for Cyber Resilience in the Eastern Partnership region
- iPROCEEDS on confiscating proceeds from online crime in South-eastern Europe and Turkey
- CyberSouth – Cooperation on cybercrime in the Southern Neighbourhood Region
- End Online Child Sexual Exploitation and Abuse @ Europe

Projects typically cover the strengthening of legislation on cybercrime and electronic evidence, including rule of law and data protection safeguards, judicial and law enforcement training, financial investigations, public/private cooperation and international cooperation.

Additional projects are in preparation and shall also be included in the object of this Call for expression of interest. All projects of the Council of Europe on cybercrime and electronic evidence are implemented by C-PROC in Bucharest by teams of project managers and other project staff.
For more information on the objectives and activities of these projects see www.coe.int/cybercrime or follow the hyperlinks above.

The purpose of this Call for expression of interest is to establish one or more lists of highly qualified consultants to support, on an ad-hoc basis, the implementation of projects, including related future projects, implemented by the C-PROC.

Through this Call for expression of interest, the Council hereby invites individuals to apply in order to be included in the list/s of qualified consultants.

When specific needs arise in the framework of the above projects, the Council may call on consultants included in the list/s. **The award of any contract in this connection shall be in accordance with the procurement procedures laid down in Rule no. 1395 of 20 June 2019 of the Council of Europe.**

Inclusion in the list/s of qualified consultants does not constitute any sort of legal commitment or obligation whatsoever, on the part of the Council of Europe, that consultancy contracts will be awarded to any of the consultants included therein.

The Council reserves the right not to launch any procurement procedure or to obtain any services needed for the purposes of the above projects from any other source at any time.

The status of staff member will not in any manner be awarded to the selected consultants, nor shall anything in this procedure be interpreted as conferring such status.

Consultants already included in the Framework Agreement 2016/AO/48 concluded with C-PROC office of the Council of Europe do not need to apply for this Call of Expression of Interest.

DESCRIPTION OF TASKS AND QUALIFICATIONS

KEY TASKS

Consultants will be expected to contribute to the achievement of project objectives and the delivery of expected results.

Tasks – depending on the area of expertise – typically include desk studies, on-site missions, training events, workshops and conferences in view of:

- Drafting legal opinions on cybercrime and providing advice to countries on the strengthening of legislation and follow up to recommendations from reviews, including data protection, human rights and rule of law requirements;

- Providing advice, through meetings and reports, on cybercrime and cybersecurity polices and strategies at technical and senior officials levels, and assessing the effectiveness of measures taken;

- Drafting analytical reports on the cybercrime situation and on measures taken by project countries on cybercrime and electronic evidence;

- Providing advice, by attending meetings and providing reports, on the strengthening or setting up of specialised (police and prosecution-type or forensic) cybercrime units, including the preparation of operating procedures;

- Conducting training courses for law enforcement officials, digital forensic experts, prosecutors and judiciary on cybercrime and electronic evidence, including training of trainers;

- Conducting training courses for cybercrime units, financial investigation units, financial intelligence units, financial sector entities and regulators, and assisting in developing cybercrime training scenarios and table top exercises;

- Designing guidelines for public authorities and financial sector operators and assisting on the development of inter-agency cooperation;

- Providing advice on the development of national training strategies on cybercrime and electronic evidence, designing or adapting training courses and manuals and assisting in the integration into national curricula;

- Providing advice, by attending meetings and providing reports, on public/private cooperation, including law enforcement/Internet service provider cooperation in line with data protection requirements;

- Assisting in the setting up of cybercrime reporting systems and elaboration of national cybercrime threats assessment reports;

- Providing advice, by attending meetings and providing reports on the strengthening of Computer Emergency/Security Incident Response Teams (CERT/CSIRT) and the cooperation with criminal justice authorities;

- Providing advice, by attending meetings and providing reports, on the strengthening of 24/7 points of contact for urgent international cooperation as well as on enhancing the efficiency of mutual legal assistance;

KEY QUALIFICATIONS REQUIRED

The consultants are expected to have (depending on the area of expertise):

- a university degree in criminal law, in international law, in computer forensics or in a related field, and extensive professional experience at international and/or national level in areas of work related to cybercrime;
- a good knowledge of the Budapest Convention on Cybercrime including the work of the Cybercrime Convention Committee and related instruments;
- a good knowledge of the functioning of computer systems and digital devices, of

conducting cybercrime investigations and collection and analyses of electronic evidence;
- proven experience and understanding of the delivery of international capacity building projects; knowledge of/experience in the implementation of EU joint projects would be an asset;
- excellent analytical, research and reporting skills;
- excellent communication and interpersonal skills;
- computer literacy;
- confirmed drafting skills in English or French are prerequisites;
- confirmed presentation and drafting skills in other languages (including Spanish, Portuguese and Russian) constitute an advantage.

FEES AND STATUS

Fees will be based on the nature of the tasks to be completed, experience and professional status.

In addition, task-related travel and subsistence expenses will be covered according to Council of Europe rules.

Contracted consultants will have to make their own arrangements for health and social insurance during the entire period of work under such contracts. They will have to declare fees received from the Council of Europe for tax purposes as required in their country of fiscal residence. Their task-related travel and stay will be covered by a travel insurance policy taken out by the Council of Europe.

SELECTION PROCEDURE

Qualified consultants will be included in one or more lists for ad-hoc consulting services covering the following subject-matter areas:

1. Legislation on cybercrime and related issues (child protection, data protection, terrorist use of information technology, money laundering, telecommunication regulations);
2. Cybercrime and cybersecurity policies and strategies and interagency cooperation;
3. Strengthening of specialized cybercrime units;
4. Law enforcement training on cybercrime and electronic evidence;
5. Judicial training on cybercrime and electronic evidence;
6. Financial investigations and prevention of online fraud and money laundering;
7. Public/private cooperation, cybercrime prevention and cybercrime reporting systems;
8. International cooperation.

For the purpose of establishing the list/s, applications will be assessed against the following criteria:

- Subject-matter expertise required
- Expertise in the legal system
- Country/region-specific expertise
- Language skills

Should the need for consultancy services arise under a project, the Council of Europe will procure such services in compliance with Rule no. 1395 on the procurement procedures of the Council of Europe. Accordingly, consultants included in the list/s of qualified consultants may, depending on the overall value of the contract, be awarded a consultancy contract directly or may be invited to submit a bid in the framework of a competitive procurement procedure.

Consultants are informed that, in the framework of such procurement procedures, the exclusion criteria included in Appendix I to Rule no. 1395 will apply.

DURATION

The short-list will be kept on file and the Council may re-launch a Call for Expression of interest at regular intervals without prior notice.

APPLICATIONS

Consultants must submit the following documents in English or French by 31 January 2020:

1 Curriculum Vitae;

2 **Cover letter**, which should indicate the

a. areas of expertise covered (one or more from among the following):

1. Legislation on cybercrime and related issues (child protection, data protection, terrorist use of information technology, money laundering, telecommunication regulations);
2. Cybercrime and cybersecurity policies and strategies and interagency cooperation;
3. Strengthening of specialized cybercrime units;
4. Law enforcement training on cybercrime and electronic evidence;
5. Judicial training on cybercrime and electronic evidence;
6. Financial investigations and prevention of online fraud and money laundering;
7. Public/private cooperation, cybercrime prevention and cybercrime reporting systems;
8. International cooperation;

b. key qualifications (see expected qualifications above);

c. average daily fee requested (excluding travel and per diem cost).

3 A sample of at least **2 relevant reports and 2 presentations** prepared by the consultant in English or French;

4 Optional: Reports or presentations in other languages (Spanish, Portuguese, Russian) if available.

Applications should be sent via email to:

Council of Europe
Cybercrime Programme Office (C-PROC)
Bucharest, Romania
cybercrime@coe.int

Only consultants included in the list/s will be contacted by the Council of Europe via email.