# Terms of Reference

# International Network of Judicial Trainers on cybercrime and electronic evidence

## I. Background and justification

As societies worldwide rely on information and communication technologies, any type of crime – not only cybercrime – may involve evidence on a computer system, that is, electronic evidence. This means that any judge or prosecutor may be confronted with cases involving such evidence. Major efforts are thus required to provide judges and prosecutors with the necessary skills, in particular through training and networking.

A concept[1] to support such efforts has been developed by the Council of Europe in cooperation with the Lisbon Network of judicial training institutions. The purpose of the concept is to help judicial training institutions develop training programmes on cybercrime and electronic evidence for judges and prosecutors and to integrate such training in regular initial and in-service training. Furthermore, a set of Principles of Judicial Training on cybercrime and electronic evidence[2] was adopted and provides a set of recommendations to be considered when defining a national strategy for judicial training on cybercrime and electronic evidence.

Joint projects of the European Union and the Council of Europe on cybercrime are supporting training through training materials on cybercrime, electronic evidence, international cooperation and online crime proceeds[3] and in priority countries a pool of national trainers has been trained to deliver training courses within judicial training institutions.

In 2019, the Council of Europe took the initiative further by discussing the feasibility and the sustainability of an international network of national judicial trainers on cybercrime and electronic evidence. The purpose is to permit trainers trained under these projects to connect, share experience and remain up-to-date.

In 2020, a second meeting aiming at shaping the mission and functions of the future community of judicial trainers was held. With this occasion it was reinforced the need for a coordinated approach towards judicial training on cybercrime and electronic evidence and the participants expressed again the support for progressing with setting up a mechanism to support the future International Network of Judicial Training and willingness to join the initiative.

## II. Mission and scope

The Network should aim at being a coordinating entity for judicial training initiatives on cybercrime and electronic evidence in regions of interest. Its mission shall therefore be defined as:

*To facilitate a common and coordinated approach to judicial training on cybercrime and electronic evidence and to strengthen professional networking of trainers.*

This should be pursued by:

---

[1] Council of Europe Cybercrime training for judges and prosecutors: a concept (other languages), October 2009: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3c3

[2] *See* https://rm.coe.int/3148-glacy-jts-principles-recommendations/1680784338

[3] Training modules are available on the CoE Octopus webpage: https://www.coe.int/en/web/octopus/training-materials

- Establishing and maintaining a pool of qualified (and possibly certified) trainers on cybercrime and electronic evidence, available for national, regional and international delivery of judicial training courses;

- Providing guidance on national judicial training strategies in the countries represented in its constituency, streamlining the Budapest Convention on Cybercrime and related standards in the national curricula of judicial and prosecutors' training institutions;

- Supporting and integrating judicial training courses of the Council of Europe on cybercrime and electronic evidence, by advising on training needs, delivery methods and relevant topics in the field, thus also providing feedback and updates to the Council of Europe judicial training strategy;

- Facilitating networking opportunities and information sharing between members, through international meetings, practitioners-to-practitioners workshops, focus groups, virtual meetings and online community tools.

## III. Governance model

The governance model of the Network is organized on three permanent entities:

## IV. Network Plenary

The Plenary is consisting of all the members of the Network and it is envisaged that it will convene once a year, in order to:

- approve annual strategy and priority plans
- set up working groups for priority streamlines
- adopt annual workplan and annual reports
- ensure there is a coordinated effort in respect to judicial training on cybercrime and electronic evidence by engaging in cooperation & collaboration with other judicial training initiatives/ networks

## V. Steering Committee

The Steering Committee is a subset of the Plenary where decisions are taken on the definition of the work plan, the development strategies and rules of engagement/ disengagement.

The Steering Committee is expected to:

- Provide guidance to the Plenary and oversee the work of the working groups
- Propose working methods
- Ensure implementation of the overall strategy adopted by the Plenary, by preparing the annual workplan and annual activity reports to be approved by the Plenary
- Prepare the quarterly progress report to be shared with the Plenary

It is envisaged to include:

- Two representatives per participating country (one representing the judicial service and training one representing the prosecution service training)
- Two representatives of the judicial experts of the Council of Europe (advisory experts to the Plenary and Steering Committee)
- Council of Europe representatives

## VI. Secretariat

The Secretariat of the Network will be ensured by the Council of Europe, through its capacity building projects on cybercrime and it is expected to:

- Maintain and update the members' list
- Ensure coordination between Steering Committee and the Network Plenary
- Perform any other administrative support as deemed necessary

The involvement and support of the Council of Europe will be re-assessed after an inception phase of three years.

Apart from its permanent bodies, it is envisaged that the Network will also operate through ad hoc working groups set up for ensuring the progress on various topics considered high-priority streams. The mandate and scope of the working groups are decided by the Plenary and their activity and working methods are overseen by the Steering Committee.

## VII. Membership

The Network shall be constituted by the following stakeholders:

- Judges, magistrates, prosecutors (and representatives from the law enforcement community) that have been formed as judicial trainers under the Council of Europe capacity building programmes on cybercrime and electronic evidence;
- Judges, magistrates and prosecutors that are vetted either by the national training institutions or national coordinator of the participating countries, according to consistent procedures that certify training skills and competencies on cybercrime and electronic evidence;
- Representatives of judicial and prosecutors' training schools;
- Judicial training experts vetted by the Council of Europe according to consistent procedures that certify training skills and competencies on cybercrime and electronic evidence.

All countries that are supported by the capacity building activities developed by Cybercrime Programme Office of the Council of Europe are invited to participate in the Network. Interested countries and relevant international organisations or institutions can become observer member until the decision to join the Network is formally taken, upon approval of the Plenary.Membership shall be reconfirmed annually, on the basis of criteria that will be established by the SteeringCommittee, and that will take into account active participation in the activities of the Network, as well asthe actual delivery of cybercrime and e-evidence courses during the year.

A minimum of one and a maximum of two focal points per country shall be set up, one responsible for judicial service training, and one for the prosecution service training. The national focal points will be reconfirmed annually, in January, by the Secretariat.

Please see also Annex 2 Privacy Statement.

## VIII. Communication and outreach

The Network will have a dedicated online area, where information will be shared on latest events and upcoming activities. The administration of the website will be taken care of by the Secretariat.

The communication with the members of the Network will be ensured by creating and using a mailing list, updated by the care of the Secretariat.

It is envisaged that the practitioners-to-practitioners' workshops will benefit of a dedicated website, set up and updated by the care of the Secretariat.

## IX. Coordination and cooperation with other international training networks

Coordination will be achieved with other international or regional training networks on cybercrime and electronic evidence, such as the Lisbon Network, CyberNet, the European Judicial Training Network (EJTN), the European Judicial Cybercrime Network (EJCN), the European Cybercrime Training and Education Group (ECTEG), INTERPOL, and any other relevant initiative in the field.

Final draft as discussed and approved during the plenary of January 2021

**Annex 1**

| 2021 Workplan of the International Network of the Judicial Trainers on Cybercrime and Electronic Evidence | | |
|---|---|---|
| Activity | Responsible | Date |
| Identify topics and members to deliver practitioners to practitioners workshops | Secretariat | By 15 January 2021 |
| Establish and maintain the list of the members of the Network | Secretariat | On a permanent basis |
| Set up of the Steering Committee | Secretariat and participating countries | By 28 February 2021 |
| First coordination call/meeting of the Steering Committee | Secretariat and Steering Committee | By end of March 2021 |
| Delivery of practitioners to practitioners workshops | Members of the Network with support of Secretariat | January to December 2021 |
| Report on the state of play of the judicial training on cybercrime and electronic evidence | Steering Committee | By 30 June 2021 |
| Second coordination call/meeting of the Steering Committee | Secretariat and Steering Committee | By 15 July 2021 |
| Identify angles for cooperation with national judicial training schools & institutes | Secretariat and national judicial training schools & institutes | By 28 February 2021 |
| Third Annual meeting of the International Network of Judicial Trainers | Plenary | By 30 October 2021 |

Final draft as discussed and approved during the plenary of January 2021

**Annex 2**

**Privacy Statement**

## 1. Who is responsible for data processing?

The Council of Europe is the "data controller" with respect to processing of personal data in relation to your enrolment and membership to the International Network of the National Judicial Trainers, which means it has the decision-making power concerning the data processing. The International Network of the National Judicial Trainers ("**Network**") is a community of national trainers, having the mission to facilitate a common and coordinated approach to judicial training on cybercrime and electronic evidence and to strengthen professional networking of trainers.

## 2. What data do we process and for what purpose?

We process personal data that we receive from you for the following purposes:

### a) Enrolment process and membership administration

To proceed with the enrolment to the Network, we need your first name, surname, e-mail address, the name of your organisation and position and the country of origin.

When you connect to the Council of Europe website (for accessing the materials we will make available in connection with the Network), certain information, such as your Internet digital address (IP), the software you use, as well as some other data are stored on the Council of Europe servers. These items do not specifically identify the user. You can find more information on the collection and use of such data in the CoE data protection disclaimer.

### c) Exchange of contact details among the participants and facilitation of access to the activities of the Network, interaction with peer members

We will draw up a list of members and we may provide it to the peer members and participating countries focal points with a view to promote professional networking. The list will contain the same data that is required for your registration in the community, that is your first name, surname, e-mail address name of your organisation, position and country of origin.

You can object to the inclusion of your data in the list of participants or specify that particular data should not be included. Should this be the case please contact us when registering your membership.

### d) Use of your e-mail address for transmitting information

We will use your e-mail address to provide you with the relevant information concerning updates on activities/events of the Network.

### e) Use of your image and voice

We will use your image and voice in order to promote the activities of the Network, in cases the activities will be recorded, with the aim of future sharing them with the members of the Network.

You can object to the use of this data or specify that particular data should not be used. Should this be the case please contact us when registering your membership.

### 3. What is the legal basis for our processing of your data?

We process your personal data on the basis of the Council of Europe's legal instruments and its internal rules in order to carry out activities necessary for the performance of the Council of Europe's tasks.

### 4. Who has access to your data?

Only those persons within the Council of Europe who support the Network's activities have access to the personal data you provide for your membership with the Network.

### 5. How do we collect and store your data?

We collect your information based on your input. We then store your information electronically on the Council of Europe's servers. We have put in place measures to protect the security of your information, including appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

### 6. How long will your data be stored?

We process and store your personal data for the period necessary to facilitate your membership with the Network, in accordance with the purposes mentioned under section 2 "2. What data do we process and for what purpose?".

### 7. Is your data transferred to a third country?

Your data is stored within the European Union and is not transferred to any country outside of the European Union.

### 8. What are your data protection rights?

You have the right to:

- request access to your personal information held by us;
- request that we correct incomplete or inaccurate personal information that we hold about you;
- request we delete or remove your personal information when there is no valid reason for us to keep it;
- object to the processing of your personal information on specific grounds relating to your situation.

If you want to exercise the above rights, or for any queries, concerns, or requests you may have in connection with the way your data is collected and used, please contact the Council of Europe by sending an email to the Council of Europe's Data Protection Officer at dpo@coe.int.