|  |  |
| --- | --- |
| Lesson: 5 – Authorisation to collect electronic evidence | **Duration: 45 Minutes** |
| **Resources required for an off-line delivery:**   * Laptop or PC running an operating system with an office suite (capable of showing pptx) * Projector and display screen * Internet access (if available) * Whiteboard * Whiteboard pens (at least 2 each of blue, black, red and green) * 2 Flipcharts with adequate paper * Student notepaper and pens * Blu tack or a similar product to allow for paper to be affixed to the walls temporarily * Files: Session 5 Authorisation to collect EE.pptx   **Resources required for an on-line delivery:**   * Laptop or PC for each trainee (if attending from home) or for a groups of trainees, depending on availability * A strong internet connection * An online tool should be provided that allows video conferencing and is specifically aimed at providing training. Due to the fact that the trainers have to stay in visual contact with the trainees, it is important that when the slides are shown, the trainers still see the trainees (in some online video conferencing tools only the slide can be seen). It is in any case also a plus to be able to provide online break-out rooms. * Files: Session 5 Authorisation to collect EE.pptx | |
| **Aim:** Through the previous training sessions, the trainees already have a picture of what the tools of the Convention on Cybercrime offer them (Session 2: Refresher Course on the Budapest Convention), the digital evidence to which these tools are applied (Session 4: Devices, Networks and Data) and the boundaries within which they should work (Session 3: Civil Liberties and Safeguards with respect to Electronic Evidence). This session will now provide a concrete legal explanation of how to obtain electronic evidence by drafting applications for prior authorisation. These applications must meet various criteria, which will be discussed in detail during this session. | |
| **Objectives:**  At the end of this session, delegates will be able to:   * Recognize particular considerations relating to the **drafting of applications** for exercise of electronic evidence procedural powers and the seeking of **prior authorisation** * Realize the **contents** of a typical application including scope & duration and other requests * Understand **what to look for** in an application seeking exercise of electronic evidence procedural powers and seeking authorisation * Understand some of the **considerations and safeguards** that should be kept in mind when drafting and looking at applications for exercise of electronic evidence procedural powers and seeking authorisation | |
| **Introduction**  The trainers have already explained in detail to the trainees, at this moment of the training, what the toolbox of the Convention on Cybercrime is, what the electronic evidence is and where it can be found and what the legal framework is within which all this should be done.  In this session it should be made clear that the exercise of the procedural powers should take place within a framework where there is a prior authorisation from the competent authorities (in most countries, a judge).  This means that the petitioner knows and is taught what the content of such a request is and why the content is relevant for, on the one hand, allowing privacy invasive measures and, on the other hand, strictly monitoring the impact of these rights.  In the first part of this session, by way of introduction, we will once again very briefly consider what is available in the Budapest Convention. What measures are interesting for obtaining electronic evidence and where are the safeguards in the Budapest Convention to allow this? It is also clarified that these safeguards are necessary and relevant throughout the process. This part can be gone through quickly, because it is a short repetition.  The second part deals with what should be included in such a petition (clearly stating that this may vary from country to country and jurisdiction to jurisdiction, but that the essence of the content should be the same). A concrete example is also shown.  It is emphasised that a request must be clear, very specific and limited in scope and duration. The second part focuses on the formal aspect.  The third part focuses on the substance of the petition and why the conditions and safeguards are contained in the petition. The focus is on the protection of privacy. Slide 39 certainly requires sufficient attention because, in addition to the protection of privacy, certain data also require special protection because they relate to the journalistic secrecy of the source, the professional secrecy of a doctor or lawyer or the freedom of religion.  All information about this session is included in the PowerPoint presentation entitled “Session 5 Authorisation to collect EE.pptx” in the resource pack. The trainer is responsible for ensuring that the materials are up to date. Changes may be made, however the objectives should be achieved. | |
| **Practical Exercises**  There is no practical exercise foreseen in this session. However, to gain more interaction from the class, the trainer could do the following (it should be borne in mind that only 45 minutes are available for this session):   * Slide 13 provides an example of a network search authorisation. This mandate is also part of the training material. This mandate can therefore be handed out and reviewed. * Trainees may comment on the extent to which they feel that this authorisation is in line with what they expect from such an authorisation, after having followed the training of this session, and with what they are accustomed to in their country from their experience. This exercise may be held at the end of the training of session 5, depending on the time still available. | |