



**UNODC**

United Nations Office on Drugs and Crime

## **Global Programme for Strengthening the Capacities of Member States to Prevent and Combat Serious and Organized Crime (GPTOC – GLOT32)**

*CASC initiative Establishing/Reinforcing the Network of Prosecutors and Central Authorities from Source, Transit and Destination Countries in response to Transnational Organized Crime in Central Asia and Southern Caucasus.*

### **Basic tips for investigators and prosecutors for requesting electronic/digital data/evidence from foreign jurisdictions<sup>1</sup>.**

- Prior to sending any request to a foreign country, make sure you have exhausted all internal/national sources of obtaining the required electronic data/evidence. Note that this data/evidence can be obtained, among other things, from open sources (i.e. publicly available information) and/or directly from Internet Service Providers (ISPs)<sup>2</sup> established/registered in your country as affiliate companies of foreign-based ISPs.
- Consider the gravity of the offence when request assistance as some countries will not execute foreign requests with regard to minor cases due to the certain limitations established by laws or practices (e. g. the U.S. will generally decline to execute any request involving less than to USD 5,000 in damages).
- Take steps to preserve electronic/digital data/evidence prior to sending the request for its disclosure as, unlike traditional evidence, various types of electronic/digital data/evidence<sup>3</sup> can be deleted permanently in a short time. For example, currently, laws of the U.S. and the majority of countries of Western Europe do not require Internet Service Providers (ISPs) to retain data for a certain time. Once deleted, data generally cannot be retrieved from an ISP. If your country and a requested country are members of the 24/7 Network (set up in accordance with article 35 of the Budapest Convention<sup>4</sup>), send the request for data preservation via your country official contact of the 24/7 Network. If your country is not a member of the 24/7 Network, send a request to a relevant investigative/prosecutorial body of the requested country. Consult with contacts of the CASC network and/or foreign liaison law enforcement officers located in your country regarding the entity to

---

<sup>1</sup> Tips were provided by participants of the SECOND INTER-REGIONAL MEETING on SHARING PRACTICES IN REQUESTING AND PROVIDING DIGITAL EVIDENCE IN ORGANIZED CRIME INVESTIGATIONS AND PROSECUTIONS, held in Tbilisi on 9-11 December 2014 in the framework of the UNODC “CASC” initiative *Establishing/Reinforcing the Network of Prosecutors and Central Authorities from Source, Transit and Destination Countries in response to Transnational Organized Crime in Central Asia and Southern Caucasus*.

<sup>2</sup> Internet Service Provider is an organization that provides services - including social networking services - for accessing, using, or participating in the Internet. For example, [Facebook](#), [Google+](#), [LinkedIn](#), [Instagram](#) and [Twitter](#) (USA); [Vkontakte](#) (Russia), [Delphi](#), [Draugiem.lv](#) (Latvia), [Hyves](#) (The Netherlands) - [http://en.wikipedia.org/wiki/Internet\\_service\\_provider](http://en.wikipedia.org/wiki/Internet_service_provider), [http://en.wikipedia.org/wiki/Social\\_networking\\_service](http://en.wikipedia.org/wiki/Social_networking_service).

<sup>3</sup> In particular, stored computer data e.g. transmission logs, subscriber information, contents of emails, and information on websites.

<sup>4</sup> The Council of Europe Convention on Cybercrime, 2001.



- which the request should be sent, the procedure/channels (i.e. informal “Police to Police” or formal Mutual Legal Assistance channel), and the content of the request. Be ready to provide (i) very basic facts of the investigation, (ii) a precise description of the data to be preserved (i.e. specific account/Internet Protocol (IP) address/website, all associated dates and times including time zones used, etc.), (iii) an explanation as to why/how the evidence sought (data to be preserved) is relevant to the investigation, and (iv) a statement that a MLA request for the data disclosure will be sent after the data is preserved.
- Given that some ISPs can accept requests for data preservation directly from foreign law enforcement/prosecutorial authorities, verify directly with the ISP in question and with the above contacts whether it is possible, and if so, send the request directly to the ISP and send a copy of the request to the above investigative/prosecutorial body of the requested country. Note that some ISPs are not “law enforcement friendly.” Therefore, consult with the authorities of the requested country before sending a request directly to an unknown ISP.
  - Verify with the requested authority whether an account holder may learn about the preservation request (either because of the ISPs’ technical design built into their servers or because the ISP notifies clients), and consider your investigative strategy accordingly.
  - Consult with your cybercrime unit about the technical aspects of the request.
  - Following data preservation, prepare your MLA request promptly. When/if available, study/use check-lists/guidance for obtaining MLA drafted by the requested country.<sup>5</sup>
  - Consult with the requested authority/authorities about the possibility of initiating/opening their own criminal investigation. Some countries won’t be able to satisfy your MLA request with regard to certain types of assistance if they don’t open their own investigations. For example, “...currently, U.S. law does not permit real time interception of the content of telecommunications or computer messages pursuant to a request for assistance concerning a purely foreign offense. Interception of communications is available only in the context of a U.S. investigation.... If U.S. and foreign authorities are investigating the same matter, it may be possible that U.S. authorities can share communications intercepted in their own investigation with foreign authorities.”<sup>6</sup>
  - The content of your MLA request depends on the types of assistance sought (i.e. electronic evidence requested), and the coercive measures needed to be taken in

---

<sup>5</sup> E.g. Requesting Mutual Legal Assistance in Criminal Matters from G20 Countries: A Step-by-Step Guide, 2012; Requests for Mutual Legal Assistance in Criminal Matters: Guidelines for Authorities outside of the United Kingdom, 2012.

<sup>6</sup> Brief Guide to Obtaining Mutual Legal Assistance in Criminal Matters from the United States (as of 25 May 2012), Section IV, Paragraph G.



the requested country. Legal requirements for satisfying foreign requests for obtaining electronic evidence vary in different countries. Generally, the more intrusive the coercive measures, the more evidence you will need to satisfy a foreign MLA request. For example, if you need to obtain the content (e.g., email messages) in an email account, you would, as a general rule, have to provide more evidence to satisfy your MLA request than you would if you only needed to obtain subscriber information.<sup>7</sup> Consult with the requested authority about the justification/grounds for your request and the circumstances under which you can obtain data/evidence (including when you request data/evidence in emergency situations).

- Indicate the need for confidentiality.
- Explain the need for urgency if you ask for an urgent execution of your request.
- Explain whether the evidence needs to be certified to make it admissible in your court, and, if so, how it needs to be certified.
- Ensure the quality of the translation of your request.
- Maintain communication with your counterpart(s) in the requested country while your request is being executed.
- Provide contact details - for both informal and formal communication – in your request.
- Be specific and proportionate. Ask only for what is really needed.
- Send/discuss a draft request before sending it via official channels.
- Ask for confirmation of the receipt of your request.
- Don't leave your request unanswered – follow-up and check with the requested authority the reasons for not responding to you.

---

<sup>7</sup> Investigative Guide for Obtaining Electronic Evidence from the United States (as of 25 May 2012) contains description of various types of stored and real-time subscriber, transactional and content information available from ISPs.