Croatia

International cooperation

Specific step-by-step procedures and best practices

Version 15 January 2021

Table of Contents

This information sheet has been prepared by the Cybercrime Programme Office (C-PROC) of the Council of Europe in view of facilitating international cooperation. It does not necessarily reflect official positions of the State covered or of the Council of Europe.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

www.coe.int/cybercrime

Back to the Table of Contents

1. Categories of Data (subscriber information, traffic data, content data)

1. Definitions under national legislation

Subscriber Information Ordinance on the Manner and Conditions for the Provision of Electronic Communications Networks and Services (Article 8)	(1) Rights and obligations arising from the subscription relationship between an operator of public communication services and end user shall be regulated by their mutual subscription contract, based upon the signed application submitted by an end user and acceptance of such application by an operator… (9) The application form referred to in paragraph 1 of this Article, determined by the operator, shall include in particular: 1. name and seat for legal persons, or name and address for applicants who are natural persons,… 6. connection point address where the subscriber shall be provided with access to public communications network, 7. address for delivery of notifications and address for delivery of bills for provided electronic communications services, 8. e-mail address at which the subsriber wants to receive notification in cases of contracted Internet access services.
Traffic Data Electronic Communications Act (Article 110)	– data necessary to trace and identify the source of a communication; – data necessary to identify the destination of a communication; – data necessary to identify the date, time and duration of a communication; – data necessary to identify the type of communication; – data necessary to identify users' communication equipment or what purports to be their equipment; – data necessary to identify the location of mobile communication equipment.
Content Data	Not directly defined under Croatian law.

Back to the Table of Contents

2. Procedures for preservation requests of stored computer data

2.1. Expedited preservation of stored computer data (Art. 29)

General remarks

Preservation requests shall be addressed to the 24/7 point of contact located at the Ministry of the Interior, Cyber Security Department. For further information please check the latest version of 24/7 contact point list.

To ensure continuously functioning (24 hours, 7 days a week), point of contact is technically equipped to send or to receive request through the network 24/7 and communicate with a competent domestic judicial authorities at any time. If necessary for the purpose of expedited preservation, a competent state attorney and investigative judge on duty are also available at any time.

Expedited preservation of stored computer data requests shall be executed according to domestic law.

Criminal Procedure Act
Article 261
(1) Objects which have to be seized pursuant to the Penal Code or which may be used to determine facts in proceedings shall be temporarily seized and deposited for safekeeping.
(2) Whoever is in possession of such objects shall be bound to surrender them upon the request of the State Attorney, the investigator or the police authorities. The State Attorney, the investigator or the police authorities shall instruct the holder of the object on consequences arising from denial to comply with the request.
(3) A person who fails to comply with the request to surrender the objects, even though there are no justified causes, may be penalized by the investigating judge upon a motion with a statement of reasons of the State Attorney pursuant to Article 259 paragraph 1 of this Act.
(4) The measures referred to in paragraph 2 of this Article shall not apply either to the defendant or persons who are exempted from the duty to testify (Article 285).

Article 263
(1) The provisions of Article 261 of this Act also apply to data saved on the computer and devices connected thereto, as well as on devices used for collecting and transferring of data, data carriers and subscription information that are in possession of the service provider, except in case when temporary seizure is prohibited pursuant to Article 262 of this Act.
(2) Data referred to in paragraph 1 of this Act must be handed over to the State Attorney upon his written request in an integral, original, legible and understandable format. The State Attorney shall stipulate a term for handing over of such data in his request. In case handing over is denied, it may be pursued in accordance with Article 259 paragraph 1 of this Act.
(3) Data referred to in paragraph 1 of this Act shall be recorded in real time by the authority carrying out the action. Attention shall be paid to regulations regarding the obligation to observe confidentiality (Articles 186 to 188) during acquiring, recording, protecting and storing of data. In accordance with the circumstances, data not related to the criminal offence for which the action is taken, and are required by the person against which the measure is applied, may be recorded to appropriate device and be returned to this person even prior to the conclusion of the proceedings.

Back to the Table of Contents

(4) Upon a motion of the State Attorney, the investigating judge may by a ruling decide on the protection and safekeeping of all electronic data from paragraph 1 of this Article, as long as necessary and six months at longest. After this term data shall be returned, unless: 1) they are related to committing the criminal offences against computer systems, programms and data (Chapter XXV Criminal Code) 2) they are related to committing another criminal offence which is subject to public prosecution, committed by using a computer system; 3) they are not used as evidence of a criminal offence for which proceedings are instituted.
(5) The user of the computer and the service provider may file an appeal within twenty-four hours against the ruling of the investigating judge prescribing the measures referred to in paragraph 3 of this Article. The panel shall decide on the appeal within three days. The appeal shall not stay the execution of the ruling.

Procedures in place

1. Confirmation of receipt
2. Legal review as to the national and international requirements
3. Sending back for additional clarifications, proceeding with the request or refusing to comply
4. In case it goes forward – obtaining the prosecutor/investigative judge order or warrant (if necessary)
5. Sending the request for execution to the provider/person possessing or controlling data
6. Upon notification from provider/person possessing or controlling data – forwarding requesting authority information whether data is preserved and if so, the name of a provider/person preserving data, case reference number, period of time for preservation and possibility of a deadline extension

Requests related to the expedited preservation are, in practice, treated as urgent.

2.2. Expedited disclosure for stored traffic data (Art. 30)

General remarks
Procedures in place

Traffic data in general include a source and destination of communication, which may be an IP address assigned to the foreign ISP. Upon the notification of domestic ISP executing the expedite preservation, Croatian 24/7 point of contact will urgently forward such information to the requesting authority.

Back to the Table of Contents

3. Procedures for mutual legal assistance

3.1. Requests for stored computer data: subscriber, traffic, content data (Art. 31)

Go to Subscriber information | Traffic Data | Content Data

General remarks

The same rules of procedure apply to obtaining subscriber, traffic and content data through MLA.

If MLA request referrs to data that have been subject to prior expedited preservation, it shall include the date of preservation, provider's name and reference number of the 24/7 point of contact.

Competent Authorities

EU countries:

Pursuant to Article 34 Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, requests shall be sent directly to the competent county state attorney's office in the form of European Investigation Order.

Non EU countries:

Central Authority responsible for mutual legal assistance and, thus receiving MLA requests is the Ministry of Justice and Public Administration of the Republic of Croatia, 10 000 Zagreb, Vukovarska Street 49.

Request for MLA may be forward directly to the competent judicial authority (court or state attorney's office) where direct communication between judicial authorities is provided in an international treaty.

Relevant contact points

There are various contact points competent to provide immediate assistance in advising on relevant domestic law, drafting requests, identifying and establishing communiciation with the person in charge for receiving requests.

The Ministry of the Interior, Cyber Security Department is designated 24/7 point of contact for the purpose of COE Convention on Cybercrime and EU Directive 2013/40/EU on attacks against information systems.

Back to the Table of Contents

In urgent cases and if there is reciprocity, the Ministry of Justice and Public Administration may forward and receive requests for MLA through Interpol and domestic judicial authorities may forward and receive requests for MLA through Interpol, with a condition that a copy of that request will be forwarded to the Ministry of Justice and Public Administration.

Depending on the countries involved, additional operational support is provided via contact points at EUROJUST, European Judicial Network, contact points established by bilateral treaties etc.

Prior consultations

Prior consultations are not necessary. However, detailed information on relevant domestic law and conditions under which MLA request will be executed could be provided by relevant contact points and authorities.

Accepted legal basis / mechanisms for MLA requests

- CoE Convention on Cybercrime
- EU Directive 2013/40/EU on attacks against information systems
-CoE European Convention on Mutual Assistance in Criminal Matters and Additional Protocols
- bilateral treaties
- reciprocy

Content of the request

Where applicable, specific requirements and form are stipulated in an international treaties.

In absence of such specific requirements, MLA request shall indicate at least:
- place of issuance and the name of the competent authority making the request,
- legal grounds to afford mutual legal assistance,
- detailed description of an act of mutual legal assistance sought and the reason for the request,
- legal title, short factual and legal description of the criminal offence,
- exact data and nationality of the person concerned and his status in the proceedings

Applicable legal requirements

Unless stipulated differently in an international treaty, investigative measures for the purpose of obtaining data shall be executed upon general requirement of reasonable suspicion that a criminal offence under Croatian law was committed and when there are no legal obstacles to the prosecution of suspect (immunity, expired statute of limitations for criminal prosecution etc.).

Confidentiality requirements

Unless stipulated differently in an international treaty, upon a request of a foreign judicial authority, the Ministry of Justice and Public Administration and the domestic judicial authority shall keep confidential the request for mutual assistance and its substance, except to the extent necessary to execute the request. If the confidentiality condition may not be upheld,

Back to the Table of Contents

the Ministry of Justice and Public Administration, i.e. domestic judicial authority shall notify the foreign judicial authority on this fact, without delay.

Urgent requests

MLA requests are, in practice, treated as urgent, though there are no legal provisions on the difference between urgent and regular requests. Due to the nature of data that need to be collected, it is accepted as common practice that all the checks are to be performed as soon as possible.

A domestic judicial authority shall act upon a request for mutual legal assistance of a foreign judicial authority even if the request was transmitted via electronic or some other telecommunications means which provide written record, if it may establish its authenticity and if the foreign competent authority is willing, upon request, to deliver a written evidence on the manner of transmission and the original request.

In case of emergency it is preferable to communicate through a relevant point of contact network.

Translation

Unless stipulated differently in an international treaty, MLA request, as well as attached documents, have to be accompanied by the translation into Croatian, and if this is not possible, into English. The translations have to be officially certified.

Limitations

Please check the grounds for refusal stipulated in an international treaties, including CoE Convention on Cybercrime.

Traffic data shall be retained by Croatian ISP for the period of twelve months from the date of the communication and shall be obtained for the purpose of evidence in criminal proceedings only for serious offences listed in the Criminal Procedure Act. In general, all offences defined in CoE Convention on Cybercrime are treated as serious offences.

3.2. Requests for real time collection of traffic data (Art. 33)

General remarks

Pursuant to Art. 109 Electronic Communications Act, all traffic data shall be already retained by Croatian ISP for the period of twelve months from the date of the communication. In practice, this exhausts the necessity of the real time collection of traffic data, although *pro futuro* recording of traffic data is legally possible.

Back to the Table of Contents

The same rules of procedure apply to MLA requests for stored data and real time collection of traffic data.

3.3. Requests for interception of content data (Art. 34)

General remarks

With the exception of confidentiality requirements and additional limitations, the same rules of procedure apply to MLA requests for stored data and interception of content data.

Confidentiality requirements

Interception of electronic data is considered to be a special collection of evidence, i.e. secret surveillance measure. It may last from three up to eighteen months, depending on the severity of criminal offence in question. The investigative judge's order on measure shall be kept in a separate cover and after the termination of the measure and even before that, may be delivered to the person the measure was ordered against if he so requests, provided that this is to the benefit of the proceedings.

Limitations

Interception of contect data shall be granted upon additional requirement that the investigation cannot be carried out in any other way or would be accompanied by great difficulties and only for serious offences listed in the Criminal Procedure Act. In general, all offences defined in CoE Convention on Cybercrime are treated as serious offences.

Back to the Table of Contents