T-CY
CYBERCRIME CONVENTION COMMITTEE
COMITÉ DE LA CONVENTION CYBERCRIMINALITÉ

T-CY(2013)17rev

Strasbourg, France
Version 27 October 2014

T-CY assessment report:
The mutual legal assistance provisions of the Budapest Convention on Cybercrime

Draft prepared by the Bureau
for consideration by the T-CY Plenary (December 2014)

www.coe.int/cybercrime

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Contents

Contact

Alexander Seger
Executive Secretary of the Cybercrime Convention Committee (T-CY) Tel +33-3-9021-4506
Directorate General of Human Rights and Rule of Law Fax +33-3-9021-5650
Council of Europe, Strasbourg, France Email: alexander.seger@coe.int

1 Introduction

Expeditious mutual legal assistance (MLA) is one of the most important conditions for effective measures against cybercrime and other offences involving electronic evidence given the transnational and volatile nature of electronic evidence. In practice, however, mutual legal assistance procedures are considered too complex, lengthy and resource intensive, and thus too inefficient.

The Cybercrime Convention Committee (T-CY), at its 8th Plenary Session (5-6 December 2012), therefore, decided to assess in 2013 the efficiency of some of the international cooperation provisions of Chapter III of the Budapest Convention on Cybercrime. At its 10th Plenary (2-3 December 2013) it decided to extend this assessment to 2014.

The Budapest Convention on Cybercrime is a criminal justice treaty. Chapter III on international cooperation refers to cooperation "for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence."[1]

The T-CY decided to focus the assessment in particular on Article 31 which provides for "mutual assistance regarding accessing of stored computer data" on an expedited basis:

> Article 31 – Mutual assistance regarding accessing of stored computer data
>
> 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.
>
> ….
>
> 3 The request shall be responded to on an expedited basis where:
>
> a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or
>
> b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

The purpose of the present Assessment is to identify solutions allowing for more "expedited" mutual assistance and to render international cooperation in general more efficient.

Article 31 is assessed in the context of the broader international cooperation regime, that is, in connection with Articles 23, 25, 26, 27, 28 and 35 Budapest Convention.

A questionnaire prepared by the Bureau of the T-CY was circulated to Parties and Observers on 18 February 2013 with a deadline of 10 April 2013. The 9th Plenary of the T-CY (4-5 June 2013) held a first round of discussions based on the compilation of replies received (see table of replies received), a second round at the 10th Plenary on 2-3 December 2013 and a third round at the 11th Plenary on 17-18 June. Additional replies or comments were received following discussions in these Plenaries.

---

[1] See Articles 23 and 25.1 Convention on Cybercrime.

The report is based on replies to the questionnaire and other comments and inputs received between April 2013 and September 2014 from the following States:

1. Albania
2. Armenia
3. Australia
4. Austria
5. Azerbaijan
6. Belgium
7. Bosnia and Herzegovina
8. Bulgaria
9. Costa Rica
10. Croatia
11. Cyprus
12. Dominican Republic
13. Estonia
14. Finland
15. France
16. Georgia
17. Germany
18. Hungary
19. Iceland
20. Italy
21. Japan
22. Latvia
23. Lithuania
24. Malta
25. Mauritius
26. Republic of Moldova
27. Montenegro
28. Netherlands
29. Norway
30. Philippines
31. Portugal
32. Romania
33. Serbia
34. Slovakia
35. Slovenia
36. Spain
37. Switzerland
38. "The former Yugoslav Republic of Macedonia"
39. Turkey
40. Ukraine
41. United Kingdom
42. United States of America

2 Assessment of frequency of mutual assistance and types of stored data

2.1 Types of data requested

Within the framework of international cooperation, the following types of information are requested from foreign authorities:

- Subscriber information[2] has been singled out in most replies as being the most often sought type of data. This includes information to identify the user of an IP address (or conversely, information on the IP address used by a specific person) or the owner of an email, social network or VOIP account as well as related technical information on the location, equipment used etc. Requests often comprise information on means of payment or billing data.

- This is followed by requests for traffic data, in particular for IP or mobile phone log files.

- Content data seems to be sought less often. Requests may be for content from emails, social networking accounts and chat messages or similar, or for illegal contents such as child abuse materials.

With respect to the underlying offences:

- Fraud and other financial crimes are referred to in almost all replies. These include all variations, ranging from credit card fraud, online payment fraud, auction fraud, phishing and other types of computer-related forgery and fraud related to traditional crimes such as breach of trust, bribery, tax evasion, money laundering and similar.

- Violent and serious crimes are offences motivating requests for data in many States. These may include murder, assault, smuggling of persons, trafficking in human beings, drug trafficking, money laundering, terrorism and the financing of terrorism, extortion and, in particular, child pornography and other forms of sexual exploitation and abuse of children.

- Offences against computer systems (illegal access, illegal interception, dissemination of malware, data interference) are also referred to in many replies.

---

[2] Defined in Article 18(3) Budapest Convention:

For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

a the type of communication service used, the technical provisions taken thereto and the period of service;

b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

- A few countries refer to defamation and libel (Philippines, Portugal, Slovakia, Turkey), xenophobia and hate speech (Bosnia and Herzegovina, Serbia), copyright violations (Moldova) or online gaming (Malta).

Preliminary conclusions:

- Mutual assistance for accessing stored computer data is not only related to offences against and by means of computers (Articles 2 to 11 Budapest Convention), but comprises the collection of evidence in electronic form in relation to any criminal offence (as foreseen in Article 23 Budapest Convention). This broad scope of cooperation is in line with Article 14.

- On the other hand, powers and procedures at the domestic level are to be established "for the purpose of specific criminal investigations or proceedings, which limits the application of the measures to an investigation in a particular case"[3]. This limitation to specific criminal investigations or specified data or communications also applies to the international cooperation provisions.

2.2 Frequency of requests

Most States were not able to provide statistics on the frequency of mutual assistance to access stored computer data. Reasons seem to include:

- MLA is increasingly decentralised and requests are sent or received directly between relevant judicial authorities and not only via central authorities. Central authorities are usually not executing requests themselves. Multiple offices may be involved in the sending or receiving of requests and in particular the execution of requests.

- No separate statistics are kept for requests for electronic evidence.

The limited availability of statistical data limits the possibility of analysis. The following data may serve for illustration:

State	MLA requests for data received	MLA requests for data sent
Albania	8 (2012)	Ca. 12 (2012)
Australia	10 (2011/12)	97 (2011/12)
Japan	11 (2013	1 (2013)
Lithuania	4-5 per year	3-4 per year
Republic of Moldova	27 (2013)	15 (2013)
Norway	37 (2012)	n/a
Romania[4]	95 (2012)	284 (2012)
Serbia[5]		55 (2008 – May 2014)
Turkey	11 (2012)	364 (2012)
USA	Hundreds of requests	Hundreds of requests

[3] Paragraph 152 Explanatory Report.
[4] Statistics provided by the the Directorate for Investigation of Organized Crime and Terrorism Offences within the Prosecution Office attached to the High Court of Cassation and Justice. It includes the requests made during investigation stage.
[5] Statistics for the Special Prosecutor's Office for High-tech Crime only.

Replies suggest that MLA is considered too complex, lengthy and resource-intensive to obtain electronic evidence, and thus often not pursued. Law enforcement authorities tend to attempt to obtain information through police-to-police cooperation to avoid MLA, even though the information thus obtained in most cases cannot be used in criminal proceedings. Frequently, authorities contact foreign (in particular USA-based) service providers directly to obtain subscriber or traffic data.[6] Often investigations are abandoned.

2.3 MLA versus police cooperation

Police-to-police cooperation for the sharing of data related to cybercrime and e-evidence is much more frequent than mutual legal assistance (the ratio seems to range from 10:1 to 50:1).

The general understanding is that:

- police cooperation is aimed at exchanging intelligence that could lead to the commencement of criminal proceedings;
- information obtained through police cooperation often cannot be used as evidence in criminal proceedings;
- the purpose of MLA is to obtain evidence for use in criminal proceedings (prosecution and court proceedings);
- in some Parties, only material received via MLA can be used as evidence in court (for example, in Australia). Others refer to the principle of the free evaluation of evidence in court (Finland, Hungary, Slovakia) and in others it depends on the specific case (Germany[7], Serbia[8]);
- for information requiring coercive/measures at the domestic level – and thus a court order – a formal MLA request is required;
- for content data, and in principle also for traffic data, a formal MLA request is required. Pending an MLA request a preservation request under Article 29 or 30 should be issued to preserve data.

[6] See transparency reports on law enforcement requests to different companies at http://www.google.com/transparencyreport/?hl=en-GB

[7] Comments by Germany: The use of information supplied through police-to-police cooperation in accordance with the EU framework decision 2006/960 is restricted to the purpose for which the information was originally transmitted. The use of information as evidence in Court requires additional approval by the state having transmitted the information.

[8] Comment by Serbia: The information gathered through police cooperation cannot be used as evidence in the proceedings, but only for the purposes of investigation. Information gathered through international police cooperation can be used as evidence as long as it is considered acceptable according to our national legislation.

With regard to data that can be shared without MLA the situation appears to be more diverse between responding States:

- Armenia can provide traffic data without MLA but upon an official request describing the case and the information needed. A court order can be obtained within Armenia if necessary.

- Australia can provide specified traffic and subscriber data for investigative purposes to foreign law enforcement on a police to police basis.

- Germany (on the basis of reciprocity), Hungary, Switzerland, Turkey can share subscriber information without an MLA request.

- Philippines can share evidence of illegal activities by foreign nationals. Philippines can provide data without MLA by principle of reciprocity.

- Data that can be obtained domestically by the police without compulsory measures and thus without court order can be shared (by Australia,[9] Belgium, Cyprus, Finland[10], France, Japan[11], Serbia, Switzerland).

- Data already obtained in domestic cases or operational data already with the police can be shared (by Albania, Belgium, Bosnia and Herzegovina, Latvia, Lithuania, Norway, Portugal, Romania, Slovenia, USA).

- Non-content data can be obtained directly with the approval of the provider by the other country (USA).

Preliminary conclusions:

- The opening of a domestic investigation following a foreign request or spontaneous information should facilitate the sharing of information without MLA or accelerate MLA.

- In joint investigations evidence may be gathered as or embedded in domestic evidence but may be shared informally during the investigation. Such sharing could be formalised later on if necessary for the purpose of criminal proceedings.

- The distinction between police-to-police cooperation and MLA is not always very clear. The same is true regarding the admissibility as evidence in court of material received via police-to-police cooperation.

- In some countries, a further differentiation may be required between MLA during the investigative stage and the trial stage. At the trial stage, evidence may require cooperation through Ministries of Justice or court-to-court cooperation, while other solutions may be possible during the investigative phase.

---

[9] Data that can be obtained domestically by the police without compulsory measures and thus without court order can be shared in certain circumstances for Australia: material obtained voluntarily by LEA for one purpose can only be used for another purpose with consent.

[10] Comment by Finland: All requests of assistance in criminal investigations phase are covered by MLA legislation and procedures in Finland. It is different question which is the competent authority to provide assistance.

[11] Comment by Japan: such data cannot be used as evidence at court proceedinds

2.4 Spontaneous information

The forwarding of spontaneous information is foreseen in Article 26 Budapest Convention:

> Article 26 – Spontaneous information
>
> 1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.
>
> 2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

Replies suggest that this possibility is used or understood by States to a very different extent:

- Never or rarely used or no experience: Estonia, France, Hungary, Japan, Lithuania, Malta, Netherlands, Slovakia, Slovenia, Spain, and "The former Yugoslav Republic of Macedonia".
- Not very often: Albania, Armenia, Bosnia and Herzegovina, Georgia, Romania, Slovakia.
- Often/very often: Cyprus (sending: 50/year, receiving: 35/year), Germany (daily), Latvia, Philippines, Portugal, Serbia, Switzerland (sending: 5-10/week, receiving: 1/month), Turkey, Ukraine, USA (all the time).

Advantages:

- Spontaneous information triggers domestic investigations in the State receiving such information (Albania, Austria, Belgium, Bosnia and Herzegovina, Bulgaria, Costa Rica, Croatia, Norway, Portugal, and USA).
- It can lead to multi-country operations (Dominican Republic).
- It can lead to MLA requests (Croatia).
- It may be used for direct agency-to-agency cooperation (Australia).
- Can be shared through foreign law enforcement liaison officers (Philippines).
- Reduces the need for MLA (USA).
- Spontaneous information on infected IP addresses allows law enforcement of the receiving country to contact service providers which will then inform their clients (France).

- Valuable information for analysis and investigation of complex organised crime (Cyprus, Georgia, Philippines, Switzerland).

- Useful for very urgent situations such as threat to life (Turkey).

Preliminary conclusion:

- Article 26 Budapest Convention seems to be underused. Those who exchange spontaneous information seem to make use of other agreements or are permitted by their own law to act without reference to an agreement.

2.5 Tables on Questions 1.1 – 1.4

2.5.1 Data requested (Question 1.1) and related offences (Question 1.2)

1.1	Types of stored data typically requested through mutual assistance (e.g. subscriber information, traffic data, content data) What type of stored data is typically requested from you? How often? Please provide statistics on frequency/quantity of requests if available. What type of stored data are you typically requesting from other countries? How often? Please provide statistics on frequency/quantity of requests if available.
1.2	Types of offences in relation to which stored data is typically requested through mutual assistance (provide statistics if available) The stored data requested from you is typically related to what type of offences? Please provide examples. When requesting stored data from other Parties, what offences are the requests typically related to? Please provide examples.

Country	**Incoming requests**		**Outgoing requests**	
	Data requested	**Types of offences**	**Data requested**	**Types of offences**
1. Albania	Subscriber information only (especially IP logs). *Frequency*: 6 requests this year, 8 requests last year.	Computer-related fraud offences	Subscriber information only. *Frequency*: ≤ 1 request/month.	Cybercrime offences. Other: fraud, counterfeiting and abuse of payment cards)
2. Armenia	Traffic data. Few requests per year.	- Computer related frauds and forgeries - Dissemination of pornographic materials, including child pornography - Credit card fraud and electronic payments - Illegal content - Blackmailing (via Internet)	About 50 requests/year on: - Log files - Social network user account information (not the content) - Customer information about certain IP address users. - Electronic payment information.	- Computer related frauds and forgeries - Dissemination of pornographic materials, including child pornography - Credit card fraud and electronic payments - Illegal content - Blackmailing (via Internet) - Dissemination of malware - Illegal access to computer system or

Country	Incoming requests		Outgoing requests	
	Data requested	**Types of offences**	**Data requested**	**Types of offences**
		- Dissemination of malware - Illegal access to computer system or network - Illegal possession of computer information		network - Illegal possession of computer information
3. Australia	ISP information, subscriber information and stored content. *Frequency*: 10 requests in one year (2011-2012)	Mainly fraud offences. Other: Foreign bribery, murder, criminal association and drug offences.	ISP information, subscriber information and stored content. *Frequency*: 97 requests in one year (2011-2012)	Mainly drugs and child sex offences. Other: Foreign bribery, murder, assault, theft, immigration, and people smuggling.
4. Austria	No statistics. The central authority deals with all kind of data.	No statistics. Fraud offences and other forms of economic crime. Rarely: Extortion or kidnapping.	No statistics. The central authority deals with all kind of data.	Similar to offences in relation to incoming requests.
5. Azerbaijan	-	-	IP Address subscriber info. Few requests by 24/7 contact points.	Cyber-attacks on critical infrastructures and hacking
6. Belgium	Primarily subscriber information and historical IP connection data	In general, requests for stored data related to terrorism or financing of terrorism, financial crime including money laundering, and fraud, including breach of trust.	Primarily subscriber information and historical IP connection data.	Belgium requests primarily data from the USA regarding the same type of offences (terrorism or financing of terrorism, financial crime including money laundering, and fraud, including breach of trust).
7. Bosnia and Herzegovina	Subscriber information mostly (IP address). *Frequency:* Few MLA requests per year; few requests by 24/7 contact points.	Unauthorised access to the electronic data processing protected system and network, computer fraud.	Subscriber information (IP address). *Frequency*: ≈ 1 request/month.	Money laundering, tax evasion, terrorism, inciting national, racial and religious hatred, discord and hostility, illicit use of the right to diffusion. Brčko District: Endangering security, bribery, offences related to electronic data processing system.

Country	Incoming requests		Outgoing requests	
	Data requested	**Types of offences**	**Data requested**	**Types of offences**
8. Bulgaria	All types of data (no statistics provided).	Mainly financial, banking and tax fraud, money laundering, phishing and child pornography.	Typically subscriber information and traffic data, financial information.	Mainly financial, banking and tax fraud, money laundering, phishing and child pornography.
9. Costa Rica	It depends on the type of investigation and offence investigated.	This depends on the specific case and offence investigated.	It depends on the type of investigation and offence investigated. (E.g. For a child pornography offence: pictures, videos, IP addresses, etc.)	It is not possible to establish a precise listing. Possible examples: child pornography, computer-related forgery or computer-related fraud, and threats using electronic services or devices.
10. Croatia	No data	No data	No data	No data
11. Cyprus	30 request per year on: - IP Address subscriber info - Upload files - Login info - Website info	- Hacking cases - Fraud	20 request per year on: - IP Address subscriber info - Upload files - Login info - Website info	- Hacking cases - Child pornography cases
12. Denmark				
13. Dominican Republic	N/A	N/A	Data to identify users or subscribers of email accounts or IP addresses	N/A
14. Estonia	No information.	No information.	No information.	No information.
15. Finland	No statistics. Mostly subscriber information, traffic data and content data.	Different types of crimes. Includes cybercrime offences, as well as homicide, child abuse and financial crimes.	No statistics. Mostly subscriber information, traffic data and content data.	Different types of crimes. Includes cybercrime offences, as well as homicide, child abuse and financial crimes.
16. France	No statistics. Subscriber information, traffic data, email addresses, judicial records, administrative files, etc.	Offences related to the automatic processing of data, Internet fraud, credit card fraud	No statistics. Subscriber information, traffic data, email addresses, judicial records, administrative files, etc.	Offences related to the automatic processing of data, Internet fraud, and credit card fraud.
17. Georgia	No statistics.	No statistics.	No examples.	No examples.
18. Germany	No statistics.	Fraud, hacking/computer	No statistics.	All types of offences.

Country	Incoming requests		Outgoing requests	
	Data requested	**Types of offences**	**Data requested**	**Types of offences**
	Mostly forensic computer images.	sabotage.	Mostly subscriber, traffic and content data from email and social network accounts.	Frequently homicide, fraud, child pornography and child abuse.
19. Hungary	Subscriber data Call traffic data	Property crime Violent crime	Subscriber data Call traffic data	
20. Iceland	Mostly subscriber information (web hosting services), IP logs/address verification. Approx. 5-10 requests / year.	Typically computer-related economic offences, fraud, computer intrusions.	Mostly subscriber information (web hosting services). Approx. 2-4 / year.	Mostly threats, smuggling of narcotics, computer fraud and sexual violence.
21. Italy	N/a.	Hacking, internet fraud, child pornography	N/a.	Cyber-attacks on critical infrastructures, hacking, internet fraud.
22. Japan	Subscriber information, traffic data, IP addresses, email content. *Frequency*: Once a year approximately.	Illegal access to computer systems; child pornography.	Subscriber information, traffic data. *Frequency*: No statistics.	Online banking fraud, online shopping fraud, creation of phishing websites, child pornography.
23. Latvia	Mostly content data, subscriber information, IP addresses, traffic data. *Frequency*: Two requests per month on average.	Typically computer-related fraud and illegal access; child pornography E.g. Use of a webpage hosting service within the country for the purpose of bogus sales.	Mostly traffic, content and subscriber data. *Frequency*: One request per month on average.	Illegal interception, computer-related fraud and illegal access; child pornography. E.g. Use of an email account to communicate with an ISP, a victim or an accomplice of credit card fraud.
24. Lithuania	Subscriber information, traffic data, forensic copies of hard drives of PC or servers' data. *Frequency*: 4-5 requests per year.	No information available.	Subscriber information, traffic data as well as content data. E.g. Child pornography case: IP addresses, copies of log files, Gmail chat messages, etc. *Frequency*: 3-4 requests per year.	Swindling, unlawful interception and use of electronic data, unlawful connection to an information system, etc. E.g. Case regarding the unlawful disposal of malicious code in computer systems connected to e-banking accounts, controlled from a server in Germany. *(See full reply for a detailed presentation)*

Country	Incoming requests		Outgoing requests	
	Data requested	**Types of offences**	**Data requested**	**Types of offences**
25. Malta	Subscriber information and traffic data (VOIP, online payments, gaming websites)	Requests are often related to online gaming casinos to seize information held by online gaming companies.	Subscriber information and traffic data including user details provided upon registration, associated online accounts, payment detail and technical information (IP address, Date, Time Stamp and Time Zone) Contents of a mailbox in cases of serious crime	
26. Moldova	Subscriber data (name, home address, e-mail, etc.); traffic data (log files).	Infringement of copyright, child pornography, illegal access to computer data, illegal interception, fraud, etc.	Subscriber data (name, home address, e-mail, etc.); traffic data (log files).	Violation of right to privacy, infringement of copyright, child pornography, illegal access and other cybercrimes, fraud, etc.
27. Montenegro	No requests so far. Subscriber information (IP address) [to be clarified]	Offences related to child pornography, unauthorised access to a protected database.	No requests so far. Subscriber information (mostly on IP addresses) [to be clarified]	N/a.
28. Netherlands	No data available.	No data available.	No data available.	No data available.
29. Norway	Mostly subscriber information, IP logs (web hosting services and other), and cell phone logs; content data as well. *Frequency*: 37 requests in 2012 (excluding telephone logs and related)	No data on IP logs from ISPs. Fraud and other financial crimes (12 requests out of 37), threats and harassment (10), child abuse images (5), computer intrusions (3), and other crimes (murder, drug offences, etc.).	No statistics on outgoing requests. Mostly subscriber information, IP logs (Facebook, Skype, web-hosting services), cell phone logs; content data as well.	Murder, serious drug offences, aggravated robberies, serious sexual offence. Other: computer crime, serious, fraud, etc. *Frequency*: No national statistics.
30. Philippines	IP address verification and subscriber information. Requests are rare.	Hacking, violation of access devices act and child pornography.	Details on accounts in Facebook, webmail or similar. Requests are frequent.	Child pornography, violence against women, child abuse and libel.

Country	Incoming requests		Outgoing requests	
	Data requested	**Types of offences**	**Data requested**	**Types of offences**
31. Portugal	No statistics. Subscriber data, list of numbers used, traffic data.	Phishing scams, paedophilia on Internet, other computer-related economic offences.	Subscriber data, list of numbers used, traffic data. E.g. IP address, time zone, etc.	Illegitimate access by hackers, defamation, data theft.
32. Romania	Subscriber information and related information (logs, location, equipment, etc.), computer data, data falling under data retention law.	Mostly computer-related offences (illegal access, data interference, child pornography, etc.), as well as electronic commerce offences. Statistics: 95 requests.	Subscriber information and related information (logs, location, equipment, etc.), computer data, data which may fall under data retention law.	Mostly computer-related offences (illegal access, data interference, child pornography, etc.), as well as electronic commerce offences. Statistics: 284 requests.
33. Serbia	Subscriber information mostly (IP logs). *Frequency*: 8 requests in four years.	Cybercrime offences.	Subscriber information (Special Prosecutor's Office for cybercrime and Police Dept.) and traffic data (only SPOC) *Frequency*: 56 rogatory letters for MLA requests in the period 2008-2013 (SPOC), 3 requests by the Police Dept. so far.	Cybercrime offences. Other: Endangerment of safety, Fraud, Counterfeiting and Abuse of Payment Cards, Instigating National, Racial and Religious Hatred and Intolerance, and Terrorism.
34. Slovakia	Only one MLA request received in 2012/13 for specific subscriber information and traffic data.	Serious bank and computer fraud.	13 requests in 2012 and 11 in the first five months of 2013 on: IP and other data to identify subscribers, traffic data, transactions with payment cards, passwords, email content.	Various types of fraud, carding and related fraud, money laundering, defamation etc.
35. Slovenia	Mostly subscriber information, as well as traffic data. *Frequency*: About 20 requests as a whole.	Typically internet fraud offences, internet threads via email, identity theft.	Mostly subscriber information, and one on traffic data. *Frequency*: 4-5 requests as a whole.	Typically internet fraud offences.

Country	Incoming requests		Outgoing requests	
	Data requested	**Types of offences**	**Data requested**	**Types of offences**
36. Spain	No statistics. Mostly subscriber information, as well as content data, hosting data and data related to electronic means of payment.	Mostly swindling, fraud, sexual child exploitation, threats, offences against integrity of the data and offences against intellectual and industrial property.	No statistics. Mostly subscriber information, as well as content data, hosting data and data related to electronic means of payment.	Mostly threats and child pornography (especially regarding subscriber or content information).
37. Switzerland	No statistics. Subscriber information (IP addresses)	Fraud, computer fraud, unauthorised obtaining of data, unauthorised access, [child] pornography, drug trafficking.	No statistics. Subscriber information, content data.	Fraud, computer fraud, unauthorised obtaining of data, unauthorised access, [child] pornography, drug trafficking.
38. "The former Yugoslav Republic of Macedonia"	Subscriber information, traffic data. *Frequency*: Only a few cases (2010-2013).	No request.	Traffic data and subscriber information. *Frequency*: 14 MLA requests, mostly traffic data. 7 requests for traffic data for child pornography and 12 cases related to identity thefts	Illegal access to computer system, offences related to child pornography, identity theft.
39. Turkey	Data on IP, location, registration, payment, other information and content. *Frequency*: 7 requests in 2011, 11 requests in 2012.	Illegal Access, hacking website, computer sabotage, computer fraud, website forgery, insulting, threat, defamation, blackmail.	Data on IP, location, registration, payment, other information and content. *Frequency*: 232 requests in 2011, 364 in 2012.	Illegal Access, hacking website, blackmail, computer sabotage, computer fraud, website forgery, threat, defamation, misuse of credit card, payment fraud, violation of privacy, violation of secrecy, illegal recording and tapping of communications, terrorism, smuggling.
40. Ukraine	(MoI) Subscriber data, log files, dumps of billing systems, copies of servers, etc. *Frequency*: 4 requests in 2013 so far.	(MoI) DDoS attacks, unauthorised access to LEA servers, theft of public authorities' data, etc. E.g. 2011, request by France following illicit intrusion into Government servers.	(MoI) Subscriber data, log files, dumps of billing systems, copies of servers, WMID owners, etc. *Frequency*: No statistics. (Sec Serv)	(MoI) All types of cybercrime offences. (Sec Serv) Involvement in international hacking teams, development of malware, intrusion

Country	Incoming requests		Outgoing requests	
	Data requested	**Types of offences**	**Data requested**	**Types of offences**
	(Sec Serv) No statistics. IP addresses, copies of hard drives, traffic data. *Frequency*: 21 requests in 2009, 18 in 2010, 11 in 2011, 28 in 2012, 11 so far in 2013.	(Sec Serv) No statistics. Cybercrime offences, financial crimes, with regional specificities.	Usually, IP user information. Frequency: 8 requests since 2006 (6 in 2009, 1 in 2011, 1 in 2012).	in banking systems, cash withdrawal of money.
41. United Kingdom	Mostly subscriber information, telephone billing and IP data. Other: Content data and real-time interception.	Any type of offences.	Mostly subscriber information, telephone billing and IP data. No statistics.	[to be clarified]
42. United States of America	Traffic data, subscriber data, hosting service content, stored email. *Frequency*: Hundreds of requests per year.	Mostly classic computer crime (credit card fraud, computer intrusion), and violent crimes (kidnapping, mass shootings, terrorism, bomb threats).	Traffic data, subscriber data, and stored email. *Frequency*: Hundreds of requests per year.	Any type of crime; mostly classic computer crime.

2.5.2 MLA versus police cooperation (Question 1.3) and spontaneous information (Question 1.4)

1.3 Mutual assistance versus police-to-police cooperation According to your law and practical experience, how do you distinguish between mutual assistance and police-to-police exchange of information regarding stored computer data? What type of information (including stored computer data) could you provide through police-to-police cooperation without or prior to a request for mutual assistance? What conditions would be attached to providing such information? 1.4 Spontaneous information (Article 26) Article 26 is about sending information to another States in the absence of a request for mutual assistance: How often do you send or receive spontaneous information? In your experience, how relevant is such information and what follow up do you give to such information? Please provide examples to illustrate the use of this possibility.

Country	MLA vs. police cooperation (Q 1.3)		Spontaneous information (Q 1.4)
	Distinction	**Data provided without MLA**	
1. Albania	Police cooperation: - is much quicker; - avoids formal requirements of MLA and the need for bilateral agreements.	Only operational data originated in police work.	- Frequency: Not very often. - Use/Relevance: To help in commencing criminal proceedings or submitting an MLA request from foreign authorities. - Follow-up: Any additional information is provided to the foreign authorities.
2. Armenia	MLA is only possible if a criminal case has been initiated. 24/7 and police-to-police to obtain sufficient information to start criminal proceedings. Most requests remain unanswered as other countries require an MLA	Traffic data can be provided without MLA upon an official request describing case and information. If the request comes without court decision, a court order can be sought within Armenia.	One urgent case 3 years ago requesting information on an SMS threatening a school. Solved within 3-4 hours.

Country	MLA vs. police cooperation (Q 1.3)		Spontaneous information (Q 1.4)
	Distinction	**Data provided without MLA**	
	request.		
3. Australia	For outgoing requests, a MLA request is necessary for data to meet Australia's admissibility requirements in domestic court proceedings. Data obtained through police can only be used for investigation purposes. For incoming requests, an MLA request is necessary where assistance involves the use of coercive powers (e.g. requests for prospective telecommunications data).	IP logs and subscriber data obtained from ISPs. In certain circumstances, the police can require the preservation of content data on behalf ofa foreign LEA, pending an MLA request.	Frequency: No statistical data. Use/relevance: Generally on an agency-to-agency basis rather than government-to-government basis. The central authority can facilitate liaison between LEA agencies.
4. Austria	An MLA request is necessary to obtain traffic data and content data.	Data that have, owing to their nature, to be transmitted under international law; Data required by foreign LEA to fulfil its duties, on condition of reciprocity; Data required by Interpol for criminal investigation.	Frequency: No statistical data. Use/relevance: Information that could lead to a criminal investigation of an offence falling under national jurisdiction is forwarded to the competent prosecutor. Follow-up: The result of the investigation (e.g. conviction) is communicated to the foreign authority which provided information.

Country	MLA vs. police cooperation (Q 1.3)		Spontaneous information (Q 1.4)
	Distinction	**Data provided without MLA**	
5. Belgium	The difference is the ultimate purpose. The purpose of judicial cooperation is to obtain evidence for use in criminal proceedings. In principle, information received or sent through police cooperation do not commit judicial authorities and cannot be used as evidence.	Police cooperation is in principle limited to the freezing of stored data. Transmission requires a rogatory letter unless the police have already obtained the data under an investigation in Belgium. If the same data are needed in another jurisdiction, the competent magistrate could authorise their transmission to foreign authorities.	If spontaneous information is received by the high-tech crime unit, a statement (PV) is prepared and submitted to the prosecution.
6. Bosnia and Herzegovina	Different legal frameworks apply. E.g. ISPs are not obliged to deliver data upon direct request by the police. Without court order.	Operational data held by the police, provided no court order is required (depending on privacy rights issues).	Frequency: No statistical data (no case under the 24/7 CP, some cases via INTERPOL channels). Use/Relevance: Whenever operative data or evidence related to a criminal offence, committed or in preparation in another State, is at disposal (mostly IP addresses). Follow-up: On any further action taken. Mandatory under domestic law.
7. Bulgaria	Data obtained through police-to-police cooperation cannot be used in court. Specific mechanisms apply for EU requests for assistance	Information and data from the Ministry of Interior information funds; Information or data, received from other state bodies or local government authorities, from legal entities and natural persons. *Conditions*: Applicable to relations with EU	Frequency: N/a. [to be clarified] Use/relevance: It depends on the information. The sharing of modus operandi, best practices, or examples is useful. The information can lead to the initiation of criminal proceedings (e.g. illicit trafficking in cultural goods, money laundering, counterfeiting currency, computer-related offence, trafficking in human beings, sexual exploitation of children, etc.).

Country	MLA vs. police cooperation (Q 1.3)		Spontaneous information (Q 1.4)
	Distinction	**Data provided without MLA**	
		Member States and signatories to the Schengen Agreement; Compliance with domestic requirements (see art. 161 e of the MoI Act new – SG 93/09).	
8. Costa Rica	The Attorney General's Office deals with mutual assistance requests. This does not exclude coordination with police organisations (e.g. Interpol)	No data can be obtained without a judicial order.	Frequency: No statistical data Use/relevance: Very high relevance, e.g. to define investigation strategies for future requests of international penal attendance.
9. Croatia	Spontaneous exchange of information is regulated in the Article 18 of the Act and it must be conducted according to the rules regulating human rights and the protection of personal data. This information might be used to initiate investigations or criminal proceedings. While the use of this data in court as evidence is not allowed without a mutual legal assistance request (letter rogatory), this is the case with incoming and outgoing requests. Stored data can be kept by the police only temporarily for 90 days (and afterwards, for extended period for another 90 days), but in order to transmit it	General information on offenders and offences (MoI database). Data from state institutions (when allowed without court order); data obtained through interviews.	Frequency: No data. Use/Relevance: Whenever the data is of help in initiating or implementing an investigation or court procedure, or can lead to the submission of a MLA request. Follow-up: On any further action taken. Mandatory under domestic law.

Country	MLA vs. police cooperation (Q 1.3)		Spontaneous information (Q 1.4)
	Distinction	**Data provided without MLA**	
	to the requesting state a formal request is needed.		
10. Cyprus	Any data not requiring a warrant in Cyprus can be provided without MLA, including IP address [does this mean subscriber info?], company registry data.	Data on company registration, criminal records and personal details, vehicles, ship owners may be given prior to a formal MLA request.	The Cybercrime Unit sends about 50 letters with such information per year and receives about 35 per year. The information is for the purposes of analysis and pro-active measures.
11. Dominican Republic	MLA if the data is to be used in judicial proceedings.	Data on IP addresses or subscriber to telephone services or on local websites if hosted in the Dominican Republic and with the help of the Public Ministry.	Information is exchanged in particular with the countries participating in the Iberoamerican Forum of cyberpolice forces (Foro Iberoamericano de Encuentro de Ciberpolicías, Fiec). This resulted in successful multi-country cooperation and the arrest of more than 25 members of Anonymous.
12. Estonia	Police cooperation applies to the exchange of data that are publicly available, or available in the State's database. MLA regards data not obtainable in the abovementioned contexts, or for which procedural actions are necessary.	Information that is publicly available or available in the State's databases.	Frequency: No statistics. Such process in allowed, but rarely used. Use/relevance: Dependent on the content and quality of information on a specific case. E.g. Information on pirated goods sold on a website, without providing details – on the goods, victims and relation to the receiving State – is of limited interest.
13. Finland	Police cooperation is mostly used to direct ongoing investigations (i.e. find the best ways to collect evidence); Mutual assistance relates to official exchange of information and requests to gather evidence. Threshold to activate mutual assistance cooperation: When the	Different type of information, for the purpose set out in Q 1.3.1. Data cannot be provided when its obtaining requires coercive measures.	Information not available.

Country	MLA vs. police cooperation (Q 1.3)		Spontaneous information (Q 1.4)
	Distinction	**Data provided without MLA**	
	criminal investigation phase begins. (It begins when there are reasons to suspect that a criminal offence has been committed.		
14. France	Mutual assistance may relate to official cooperation (through Interpol, Europol or G8 channels), to be used in judicial investigation and proceedings; Police cooperation (via liaison officers or other) is more informal. It may provide indications for investigations. Evidence cannot be used as such in proceedings.	Any data which does not require the issuance of a judicial order or the undertaking of a coercive measure.	Frequency: Very rare. Example: Information provided by Germany on compromised servers, including a list of clients' IP addresses. The hosting provider was contacted and was provided with the list of clients in order to inform them.
15. Georgia	Mutual assistance is regulated by the law on cooperation between judicial authorities; Police cooperation is regulated by the law on cooperation between LEA.	Data contributing to the prevention, detection and suppression of crimes; data on persons wanted, participating or suspected to participate in a crime; offenders' connections, structures, modus operandi, etc.; acquisition and registration of firearms; identification of a motor vehicle and its owner/user; criminal intelligence, etc.	Frequency: No statistics. Used on certain occasions. Use/relevance: (Sending) Valuable whenever LEA consider the information as valuable for the foreign State, provided that transmitting the information is compatible with domestic legislation; (Receiving) Very valuable for the investigation of complex crimes (e.g. transnational organised crime), either to give a certain direction to investigations, or to provide additional evidence to bring a suspect to justice.
16. Germany	Data needed for criminal proceedings requires a mutual assistance request.	Subscriber data, on condition of reciprocity.	Frequency: Information sent on a daily basis; reception of information as well (no statistics available).
17. Hungary		Subscriber data can be handed over without MLA request.	No experience. Never sent or received such a request.

Country	MLA vs. police cooperation (Q 1.3)		Spontaneous information (Q 1.4)
	Distinction	**Data provided without MLA**	
18. Iceland	Data needed for criminal proceedings requires a mutual assistance request.	A wide range of information when a related domestic investigation is ongoing. Also intelligence information	Such information is usually forwarded on police level and not through Ministry. Therefore, no information available.
19. Italy	Distinction based on the informal character of the request.	N/a.	Use/relevance: Only regarding information on cyber attacks or threats. It does not involve stored data. Example: Information on the planning of a cyber attack by a group of hackers is transmitted, after verification, to the target system or network.
20. Japan	Use of mutual assistance when the request involves the provision of evidence or compulsory measures; Police cooperation for other cases.	Data not amounting to the provision of evidence, and for which compulsory investigation is not required.	No practice.
21. Latvia	Police cooperation is necessarily followed by mutual assistance, if stored computer data is to be used as evidence.	Information from State's databases (e.g. criminal records, personal information), data on IP addresses or subscriber to telephone services	Frequency: Very often. Example: Information on money "mules". Follow-up: Usually, initiation of investigations.
22. Lithuania	Information obtained through the channels of (international) police cooperation is used for police intelligence purposes. Exception: When the foreign provider of information allows the use of the data as evidence.	Any type of information, including stored computer data, which is not prohibited to collect and provide without official permission of the prosecutor or the court and pursuant to other provisions of national law.	No practice.
23. Malta			Spontaneous information is rarely sent/received. If so through channels such as Europol or Interpol, and once through 24/7 point of contact. It is usually related to child abuse materials downloaded or users

Country	MLA vs. police cooperation (Q 1.3)		Spontaneous information (Q 1.4)
	Distinction	**Data provided without MLA**	
			whose computers are infected with malware. Often the information is sent after the 6-month data retention period and the necessary data is no longer available and thus the uses cannot be identified anymore.
24. Moldova	All requests in criminal prosecution are addressed to the General prosecutor. All requests made during trial or execution of a sentence are addressed to the Ministry of Justice.	Only operational data originated in police work.	N/a.
25. Montenegro	No data.	Any data, depending on the criminal offence and requirements of domestic procedural law.	Frequency: No data. Use/Relevance: N/a.
26. Netherlands	The prosecutor's office is in charge of MLA request to obtain stored computer data. Preservation requests are received through the 24/7 point of contact. Requests for transfer of preserved data are received through AIRS (central authority) or the IRC (office for international legal assistance in criminal matters).	Data preserved by order of the prosecutor may be shared through police cooperation pending a formal request, but only for investigative purposes and with consent of the prosecutor (very urgent cases only); Data preserved by order of the investigative judge can only be formally transferred with consent of the competent court.	Sending information: Frequency: Approx. 3 times per month. Use/relevance: Action is as quick and elaborated as possible, given the high dependency of the beneficiary State on the information provide. Receiving information: Frequency: Almost never, possibly because of legal obstacles. Use/relevance: No sufficient practice.
27. Norway	Exchange of content data generally requires a mutual assistance request; Possible to exchange certain data through police cooperation (e.g.	A wide range of information, when a related domestic investigation is ongoing; Certain information (e.g. intelligence).	Frequency: No statistics. Use/relevance: Can be of importance in many cases, as intelligence information (modus operandi) or to initiate criminal investigations;

Country	MLA vs. police cooperation (Q 1.3)		Spontaneous information (Q 1.4)
	Distinction	**Data provided without MLA**	
	subscriber information) without a formal request nor a court order, but easier in case of mutual or parallel investigations.		Example: Information on a malware discovered in the course of criminal investigations of computer intrusions. Can be channelled through Europol and similar mechanisms. Follow-up: Dependent on the information (e.g. relevance for a current case/project)
28. Philippines	Mutual assistance is utilized whenever evidentiary documents from foreign jurisdiction is needed for the successful prosecution of cases being filed in the country or under investigation whereas intelligence gathering is done whenever information from other jurisdictions is useful in identifying and determining the involvement of any suspect in illegal acts or basically for case build up. Police cooperation is done following an official request but without necessitating judicial intervention. The data shared however, are restricted and cannot be used as evidence in any proceedings without prior consent from the Requested State.	Only proofs of illegal activities of foreign nationals and intelligence reports. Stored computer data require court orders, hence, cannot be used by other jurisdictions without undergoing the mutual assistance requirements. Informational data and intelligence reports. Stored computer data require court orders, hence, cannot be used by other jurisdictions without undergoing the mutual assistance requirements.	Spontaneous information is often received from the locally assigned police attaches of foreign jurisdiction. Intelligence gathering and sharing, is not just about requests for information, there is always a close cooperation and coordination between the Department of Justice of the Philippines and the police and the police attaches of different countries.
29. Portugal	The obtaining of data is subject to the approval of the judicial	None.	Use/relevance: Any police information is transmitted, provided that it does not require a judicial request. Information received is of great

Country	MLA vs. police cooperation (Q 1.3)		Spontaneous information (Q 1.4)
	Distinction	**Data provided without MLA**	
	authority.		importance and often leads to the opening a criminal case.
30. Romania	Different legal frameworks apply; legal provisions on judicial cooperation prevail over provisions on police cooperation; Police cooperation focuses on requests for exchanging operational data, information on offences, etc.; Police cooperation is often needed at an earlier stage of investigations.	Personal data from domestic databases (e.g. criminal records) information, intelligence held in police databases	Frequency: Not very often. Use/relevance: Requests are sent/received on the basis of applicable international agreements. Requests received on the basis of the MLA Convention of 1959 are analysed and forwarded by the central authorities to the competent judicial authorities (local prosecutor's office). Need for more experience to evaluate this tool. Example: Information received on a computer-related fraud case committed by a national, forwarded to the Prosecutor's Office attached to the High Court of Cassation and Justice.
31. Serbia	Police cooperation: is much quicker; avoids formal requirements of MLA and the need for bilateral agreements.	Operational data held by the police, provided no court order is required.	Frequency: Very often. Use/Relevance: Whenever information on criminal activities can be of interest for foreign authorities and vice versa. Follow-up: Any additional information is provided to the foreign authorities.
32. Slovakia	MLA requires criminal proceedings. On the contrary, police cooperation may be understood as cooperation between police authorities aiming at obtaining the information needed for police in order to perform its tasks and such information, which could lead to commencement of criminal proceedings. Results of police cooperation, however, cannot be used as evidence in criminal proceedings.	Only criminal intelligence information may be exchanged by police. It should be noted that access to traffic/content data, IP addresses, logs (etc.) in criminal proceedings is regulated. Such data is covered by telecommunication secrecy regulated by a separate act. In criminal proceedings, access to such data requires judicial authorization.	So far Article 26 Budapest Convention is not used for exchanging spontaneous information, but sooner or later it will be used as is the case with similar provisions in other treaties.

Country	MLA vs. police cooperation (Q 1.3)		Spontaneous information (Q 1.4)
	Distinction	**Data provided without MLA**	
33. Slovenia	Data obtained via police cooperation requires a validation before can be used in court as a evidence.	Information from the State's databases; information already obtained in some domestic cases.	Frequency: Very rare. Use/relevance: It may allow the opening of a new case, when the information characterises an offence in domestic law. Additional evidence may be used in criminal proceedings.
34. Spain	Mutual assistance is carried out by judicial authorities in the framework of judicial proceedings; Police cooperation regards police investigation (i.e. before the initiation of proceedings).	Only technical data related to connexions.	Frequency: No experience. Use/relevance: Such information would be immediately forwarded to the competent prosecution office. At the police level, it may trigger the initiation of investigations (especially in cases of fraud, cyber attacks and child pornography).
35. Switzerland	Mutual assistance regards the handling of requests from judicial authorities and entailing compulsory measures [to be clarified] Police cooperation regards the handling of requests from police authorities from their own competence and not compulsory at the procedural level (subscriber information, etc.)	Data regarding holders of IP addresses and fringe technical data which are available without compulsory measures; (In general terms) No restriction as to the type of data that can be transmitted, provided it concerns the fight against crime and respects fundamental rights and principles of national laws.	Frequency: No statistics. 5-10 sending per week on child pornography, approximately one reception per month. Use/relevance: Information sent is mainly about child pornography. (E.g. Ads regarding websites containing such content). Information received regards mostly either the modus operandi of criminal group (e.g. Information send by Interpol Moscow on a romance scam called *Russian bride*), or information on a specific criminal case, allowing LEA to anticipate an offence (e.g. FBI information on a denial of service attack in preparation) or to initiate investigations (e.g. Child pornography websites host in the country)
36. "The former Yugoslav Republic of Macedonia"	Police cooperation and MLA are highly interconnected, especially in urgent cases.	Only to establish the availability of the data and the type of data.	Frequency: No cases. Use/Relevance: Very valuable to solve cases where computer stored data is essential; saves time when the data is particularly fragile.
37. Turkey	[to be clarified]	Only subscriber information. (Traffic data and content data require the approval of judicial authorities.)	-Frequency: No data. This practice is not rare. -Use/Relevance: Assistance of foreign judicial authorities; transmission of criminal intelligence in urgent (life-threatening) cases, for police use only.

Country	MLA vs. police cooperation (Q 1.3)		Spontaneous information (Q 1.4)
	Distinction	**Data provided without MLA**	
38. Ukraine	(MoI) Exchanging data is only possible through mutual assistance; -Preservation of data can be requested by the Cybercrime Division of the MoI. (Sec Serv) Information obtained via mutual assistance can be used as evidence in court.	(MoI) No data can be obtained without a court order from ISPs or other legal/natural persons. (Sec Serv) Only information that does not contain personal data or related data.	(MoI) Information can be sent, if it does not infringe rights of private persons, the secrecy of private data holders, and law on State secrecy. Use/relevance: May be very relevant (analytical data received from open source, statistical data processed by cybercrime units, etc.) (Sec Serv) Frequency: Regular sending of information, mostly on fraud cases. Regular request for information as well (40-70 requests per year). Use/relevance: Information is relevant whenever it regards illegal activities of nationals or is requested by a partner.
39. United Kingdom	MLA follows formal rules of mutual assistance; Police cooperation sharing is for intelligence.	Data accessed via police to police cooperation. [to be clarified]	Frequency: Not available. Follow-up: No follow up unless further requests are made. The validity and proportionality of the request is checked.
40. United States of America	Mutual assistance is needed whenever a court order is required to obtain the data. (*See right column for details*)	Preservation may be obtained through the police or directly by the foreign authority; Non-content information can be obtained directly with the approval of the provider; Information already obtained in domestic investigation or prosecution, subject to limitations; Content information, with the assistance of domestic LEA, in case of emergency and with the approval of the provider.	Frequency: All the time, although it is not necessarily labelled as such. Use/relevance: Useful. This label is used to provide potentially helpful information without requiring an MLA request by the foreign State; It may minimise the need of an MLA request, given that part of the information needed has already been passed to the foreign State.

3 Assessment of procedures and requirements for mutual assistance regarding accessing stored data

3.1 Requirements

Replies to the questionnaire list a number of requirements.

Form of the request:

- Written form or in electronic form provided that its authenticity can be established.
- Language requirements foreseen in the legal instrument (see below).
- Transmission by means and through authorities foreseen in the legal instrument on which the request is based.

Content of the request:[12]

- Name and contact details of the requesting authority.
- Legal basis for the request (typically domestic laws on international cooperation in criminal matters and criminal procedure law in conjunction with bi-lateral agreements on mutual legal assistance, Budapest Convention on Cybercrime, European Convention on Mutual Legal Assistance in Criminal Matters and other Council of Europe treaties; United Nations and other international treaties, or reciprocity).
- Purpose and reasons of the request.
- Necessity of the request.
- Identification of the offence and applicable law (including applicable penalty).
- Summary of the facts and charges.
- Information on persons involved.
- Measures that are requested (Philippines: description of the procedure to be observed in the execution of the request).
- Description of the evidence sought and related information (the stored data sought and relationship to the offence, telephone numbers or IP addresses involved; means of the electronic communication, time period for which data is requested, etc.).
- Identification of the physical or legal person holding the data sought.
- Presence of officials from the requesting state in the execution of the request (Philippines).
- Attachment of court decision, such as for disclosure of content data.
- Relevant information for consideration of a possible intrusion into the privacy of third parties and plans to minimise this (UK).

Domestic requirements:

- Compliance of the request and measures to be taken with domestic law, in particular with respect to coercive measures.
- Dual criminality principle (Finland[13], Georgia, Germany; Hungary; Japan; Norway; Serbia; Switzerland; USA infrequently).

---

[12] See also the enumeration in Article 29 Budapest Convention.

[13] Comment by Finland: As a main rule dual criminality principle is applied in Finland, if coercive measures are required

- Request must be related to serious crime (Spain).
- "Probable cause" principle for request for content data (USA).
- Court order or decision by prosecutor, depending on the type of data requested.

The following table illustrates the institution that can authorise access to stored data at the domestic level following a foreign request for MLA.

Authorisation for access to stored computer data upon a foreign MLA request[14]

[T-CY delegations to complete the table]

State	Subscriber data	Traffic data	Content data
1. Albania			
2. Armenia			
3. Australia	Police	Police	Judicial officer (following authorisation by Attorney-General)
4. Austria			
5. Azerbaijan	Court	Court	Court
6. Belgium	Prosecutor	Court	Court
7. Bosnia and Herzegovina	Court	Court	Court
8. Bulgaria			
9. Costa Rica			
10. Croatia			
11. Cyprus			
12. Denmark			
13. Dominican Republic			
14. Estonia	Police	Prosecutor	Court
15. Finland	Police/court	Court	Court/ Police[15]
16. France			
17. Georgia			
18. Germany	Police (also Prosecutor/Court)	Court (In exigent circumstances: also the Prosecutor)	Court (In exigent circumstances: also the Prosecutor)
19. Hungary	Police	Police	Court
20. Iceland			
21. Italy			
22. Japan	Police/Court	Court	Court
23. Latvia	Prosecutor/Court	Prosecutor/Court	Prosecutor/Court
24. Lithuania	Police (also Prosecutor/Court)	Court (Prosecutor's decision approved by the Pre-trial Investigation Judge)	Court
25. Malta			
26. Moldova	Prosecutor	Court	Court

[14] Simplified table. For details see replies to questionnaire.

[15] Police authorities can seize a document. This is different than getting content of messages where a court decides.

27. Montenegro			
28. Netherlands			
29. Norway			
30. Philippines	Court	Court	Court
31. Portugal	Prosecutor (police in urgent cases)	Court	Court
32. Romania	Court	Court	Court
33. Serbia	Prosecutor	Court	Court
34. Slovakia	Court, more precisely President of the Court Chamber (before the initiation of the criminal investigations) or Prosecutor (within the preparatory proceedings), since the Slovak Criminal Code (No. 301/2005 Coll. as amended) does not differ between subscriber information and traffic data.	Court, more precisely President of the Court Chamber (before the initiation of the criminal investigations) or Prosecutor (within the preparatory proceedings)	Court
35. Slovenia	Police/Court	Court	Court
36. Spain			
37. Switzerland			
38. "The former Yugoslav Republic of Macedonia"			
39. Turkey			
40. Ukraine			
41. United Kingdom			
42. United States of America	Court (unless ISP provdes data voluntarily)	Court (unless ISP provides data voluntarily)	Court

3.2 Grounds for refusal

The Budapest Convention refers to grounds for refusal to cooperate in Articles 25 and 27:

Article 25 – General principles relating to mutual assistance

4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws. [16]

Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

---

[16] Extract of the Explanatory Report:
"259. Paragraph 5 is essentially a definition of dual criminality for purposes of mutual assistance under this Chapter. Where the requested Party is permitted to require dual criminality as a condition to the providing of assistance (for example, where a requested Party has reserved its right to require dual criminality with respect to the preservation of data under Article 29, paragraph 4 "Expedited preservation of stored computer data"), dual criminality shall be deemed present if the conduct underlying the offence for which assistance is sought is also a criminal offence under the requested Party's laws, even if its laws place the offence within a different category of offence or use different terminology in denominating the offence. This provision was believed necessary in order to ensure that requested Parties do not adopt too rigid a test when applying dual criminality. Given differences in national legal systems, variations in terminology and categorisation of criminal conduct are bound to arise. If the conduct constitutes a criminal violation under both systems, such technical differences should not impede assistance. Rather, in matters in which the dual criminality standard is applicable, it should be applied in a flexible manner that will facilitate the granting of assistance."

6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

In their replies, States list as grounds for refusal:

- The grounds listed in Article 27 Budapest Convention.
- The request does not meet formal or other requirements (see previous section).
- The request is motivated by race, religion, sexual orientation, political opinion or similar.
- The request concerns a political or military offence.
- Cooperation may lead to torture or death penalty.
- Granting the request would prejudice sovereignty, security, public order or national interest or other essential interests.
- The person has already been punished or acquitted or pardoned for the same offence ("*Ne bis in idem*").
- The investigation would impose an excessive burden on the requested State or create practical difficulties.
- Granting the request would interfere in an ongoing investigation (in which case the execution of the request may be postponed).
- Risk of discriminatory prosecution (Netherlands).
- The request is related to freedom of expression (USA).
- Proceedings do not comply with the European Convention on Human Rights (Portugal).
- The data requested is related to national security (Slovenia).
- The offence falls under military law and not under ordinary criminal law (Philippines).

Preliminary conclusions:

- Some States may refuse cooperation if the case is minor or put an excessive burden on the investigating authorities. The problem is that thus thresholds are not formalised and are not transparent to other Parties. While the resources required to cooperate in minor cases may at times be unproportional, minor cases may be part of larger cases or related to criminal organisations. More transparency and dialogue with the requesting Party is thus required if thresholds are applied.

- As indicated above, a number of Parties require dual criminality with regard to mutual assistance requests for stored computer data. Pursuant to Article 25.5 Budapest Convention and Paragraph 259 Explanatory Report, Parties are encouraged to apply a flexible approach when applying dual criminality, in particular in relation to offences under Articles 2 to 11 Budapest Convention.

- Some Parties refuse to cooperate regarding certain content matters, such as hate speech.

3.3 Language of the request

The question of language of international requests for mutual assistance is considered a major problem by most States. The main problems in this respect are:

- the delays caused by translations;
- the cost of translations;
- the limited quality of translations, including unclear terminology;
- limited foreign language skills of practitioners.

Even if for domestic purposes (legal and practical reasons) certified translations would still be required, most States accept a request in English.

Exceptions are Costa Rica (Spanish), Dominican Republic (Spanish), Germany (German), Japan (Japanese), Slovakia (Slovak), Spain (Spanish) unless other languages are foreseen under different agreements.

Preliminary conclusions:

- An additional Protocol to the Budapest Convention could stipulate that mutual assistance requests sent in English are accepted by the Parties, at least in urgent cases.

- Harmonisation of MLA requests on cybercrime and electronic evidence:

  - use of standard format would reduce need for translation (standardised headers or fields would not require translations);

  - use of a multi-language glossary for technical terms would improve quality of requests.

State	Language required or accepted[17] when receiving MLA requests
1. Albania	Albanian, English
2. Armenia	English, Russian, Armenian
3. Australia	English
4. Austria	German, English or French
5. Azerbaijan	English, Russian, Turkish
6. Belgium	English
7. Bosnia and Herzegovina	Bosnian, Croatian or Serbian, English tolerated for Interpol channel
8. Bulgaria	Depends on agreement
9. Costa Rica	Spanish
10. Croatia	Croatian, English
11. Cyprus	Greek and English
12. Denmark	
13. Dominican Republic	Spanish
14. Estonia	Estonian, English
15. Finland	Finnish or Swedish (requests in other languages may be executed if otherwise possible. Could be accepted by a decree). Also English accepted in practice
16. France	French, English
17. Georgia	Georgian, English, French, Spanish
18. Germany	German
19. Hungary	English
20. Iceland	
21. Italy	
22. Japan	Japanese
23. Latvia	Latvian
24. Lithuania	Lithuanian, English, Russian
25. Malta	
26. Moldova	Moldovan, English
27. Montenegro	Montenegrin, English, French
28. Netherlands	Dutch, French, English, German
29. Norway	English, Norwegian, Swedish, Danish
30. Philippines	English
31. Portugal	Portuguese (unless foreseen otherwise)
32. Romania	Romanian, English, French
33. Serbia	Serbian, English
34. Slovakia	Slovak
35. Slovenia	English
36. Spain	Spanish
37. Switzerland	German, French, Italian, English
38. "The former Yugoslav Republic of Macedonia"	No specific requirement. Language of requesting state accepted.
39. Turkey	Turkish, English in urgent cases
40. Ukraine	Language of the requesting State, English
41. United Kingdom	English
42. United States of America	English

[17] Bi- or multilateral agreements may provide for different language requirements.

3.4 Procedure for sending/receiving requests

The procedure for requesting mutual assistance and sending an MLA request typically involves:

1. A request for mutual assistance is prepared by the prosecutor or enforcement agency responsible for an investigation.
2. The prosecutor or enforcement agency sends the request to the central authority for verification (and translation if necessary).
3. The central authority (Ministry of Justice, Attorney-General's Department or General Prosecution Office) submits the request either
   - to the foreign central authority, or
   - directly to the requested judicial authority.

The procedure for receiving and executing requests typically involves:

1. Receipt of the request by the central authority.
2. Examination against formal and legal requirements (and translation if necessary).
3. Transmission to competent prosecutor or enforcement agency to obtain court order.
4. Issuance of a court order.
5. Prosecutor orders law enforcement (e.g. cybercrime unit) to obtain data.
6. Examination of data obtained against MLA request, which may entail translation or using a specialist in the language.
7. Transmission to requesting State via MLA channels.

If requests do not meet requirements, the process may include additional loops. An MLA request may also be accompanied by a parallel request for data preservation.

Replies suggest a number of variations:

- Between EU countries requests may be sent directly to the authorities requested (not via central authorities).
- Bosnia and Herzegovina, France: use of INTERPOL channels for MLA requests.
- Estonia: in urgent cases, requests are submitted via Interpol channels or a Schengen notice can be executed with the approval of the Public Prosecution Office, before a formal MLA request is received by the Ministry of Justice.
- Germany: preliminary contact by 24/7 point of contact with foreign counterparts in view of a possible initiation of a domestic investigation;
- Japan: if the request is not based on an MLA agreement but on reciprocity, the request is sent via diplomatic channels.
- Norway: the MLA request may be accompanied by court ruling that domestic requirements are met to obtain the data.
- Philippines: Cooperation by reciprocity is via diplomatic channels; by treaty directly between the Department of Justice and the foreign counterpart.
- Serbia: contact of foreign authorities to verify whether data may be obtained without a formal MLA request.
- Slovenia: requests may be sent or received by International Police Cooperation Sector (IPCS).

Preliminary conclusions:

- The possibility of direct cooperation with foreign judicial authorities appears to be underused – except between EU member States. This limited use also seems to be the case for Parties to the 2nd additional Protocol to the Convention on Mutual Legal Assistance in Criminal Matters (ETS 182) of the Council of Europe.
- It may be worth to consider including the possibility for direct cooperation in a Protocol to the Budapest Convention on Cybercrime.

- It may be worth to consider simplifying legal and formal requirements in a Protocol to the Budapest Convention while maintaining safeguards and requirements for coercive measures.

- Early contacts with counterparts in the requested Party are encouraged in view of initiating domestic procedures in that State.

3.5 Problems encountered

Replies list the following problems that are encountered in the MLA process:

- Time, workload and the complexity of procedures required to prepare or execute MLA request (Albania, Belgium, Cyprus, Finland, France, Italy, Japan, Moldova, Philippines, Romania, Serbia, Slovenia, Turkey, and USA).

- Delays (6 – 24 months) in responses to requests in general or in relation to specific countries (Albania, Australia, Belgium, Croatia, Dominican Republic, Finland, Latvia, Norway, Romania, and Serbia).

- Delays in providing subscriber data (Germany).

- Refusal to cooperate for "petty" offences by some countries (Austria, Costa Rica, France, Romania).

- Refusal to cooperate or no reply by some countries (Bulgaria, Estonia, Slovenia).

- Problem of cooperation with 24/7 contact points (Turkey).

- No receipt that MLA request has been received or that data has been preserved (Switzerland, UK).

- Unclear criteria for "urgent" requests (Switzerland).

- Problem of language, quality of translation, terminology used (Turkey, UK).

- Requests received too broad, for a large amount of data (Netherlands, Spain).

- Discrepancies between legal systems, such as regarding investigative powers (Albania, Moldova, Norway, Romania, Serbia, Ukraine).

- Legal restrictions (data protection) (Albania, France, Moldova, Serbia).

- Refusal of cooperation by foreign State without MLA request. However, MLA request requires sufficient information and evidence which cannot be obtained without cooperation by foreign State (vicious circle) (Armenia, Belgium).

- Request may not meet legal threshold or formal requirements of the requested State or request not complete or threshold/standard required too high (Australia, Austria, Finland, Germany, Lithuania, Slovakia, USA).

- Inadequacy of laws to permit countries to assist others (USA).

- Dual criminality requirement not met (Serbia).

- MLA request not preceded by preservation request to ensure that data is still available (Australia, Slovakia).

- Data not preserved in foreign State in spite of preservation request (Estonia).

- Data not available anymore in foreign or own State (Georgia, Italy, Norway, Portugal, Romania, Switzerland).

- Different policies by providers to make data available (Belgium).

- Contact person in emergency cases or the competent authority in foreign State not known (Bosnia and Herzegovina, Georgia, and Netherlands).

- Challenging to identity the authority concerned, e.g. web hosting provider (Norway).

- Overburdened by too many requests (Cyprus, USA).

- Limited technical skills and understanding regarding electronic evidence in requested State (USA).

- Limited power of judicial police (Portugal).

- "Probable cause" threshold.

Preliminary conclusions:

- Direct contact with foreign authorities should be sought to seek advice on requirements before sending MLA request (Australia) or to make a preservation request or initiate a parallel investigation (Norway).

3.6 Tables on questions 2.1 – 2.5

3.6.1 Requirements and grounds for refusal (Questions 2.1 – 2.3)

2.1 Requirements to be met for executing a request for mutual assistance

When receiving a request for stored computer data, what formal, legal or other requirements must be met so that you are able to execute the request? Please provide examples, including examples of requests you had to decline.

What is the legal basis allowing you to execute such a request? Please append the text of relevant legal provisions.

2.2 Grounds for refusal to cooperate

Requested Parties may refuse cooperation in certain circumstances (see, for example, Articles 25.4 and 27.4 Budapest Convention). Please list grounds for refusal and give examples of requests that you refused to execute.

2.3 Language of the request

When receiving requests, what are your requirements regarding the language?

How important is the problem of translations from and to foreign languages in terms of time, money and quality? What solutions would you propose to alleviate such problems?

Country	Requirements (Q 2.1)	Grounds for refusal (Q 2.2)	Language of the request (Q 2.3)
1. Albania	Content of the request: description of actions to be taken; reasons for submitting the request; other relevant data. Compliance with the applicable procedure, including requirements for the issuance of a	Grounds specified by the Cybercrime Convention, applied to requests from Parties to the Convention. Grounds to refuse requests from non-Parties: Requested action is prohibited expressly by law or contradict the fundamental principles of the	Required: Albanian. Tolerated: English. *Problems and solutions*: Financial burden and time required for translating requests (especially for

Country	Requirements (Q 2.1)	Grounds for refusal (Q 2.2)	Language of the request (Q 2.3)
	court order.	Albanian rule of law; Considerations regarding race, religion, sex, nationality, language, political beliefs or the social state may have a negative influence on the performance of the process [to be clarified]; No sufficient guarantee against "encroachment" of a cited person (witness, expert, defendant); No guarantee of reciprocity given by the requesting State.	native languages). Suggestion: Favour English in MLA communications.
2. Armenia		Grounds for refusal are described in the CPC of RA. In addition, a request cannot be completed if the information is insufficient or the requested information not available.	English, Russian, Armenian
3. Australia	Compliance with the conditions allowing the Attorney General ("AG") to authorise a LEA to apply for a stored communications warrant (request by the foreign authority to the AG to arrange for access to stored communications; investigation has commenced in the requesting country; offence is punishable by a maximum penalty of a certain level – *see* legislation –; reasonable grounds to believe that relevant stored data are held by the carrier); The judicial authority may then issue the warrant to the police officer on certain conditions (completion of the application process; reasonable grounds to suspect that a particular carrier holds the stored data sought; information likely to be obtained by this data access would be likely to assist with investigations initiated by foreign authorities).	*Mandatory* grounds (applied by the Attorney General): The request concerns: a political offence or a related offence; a purely military offence; Substantial grounds to believe that the request was made on account of a person's race, sex, sexual orientation, religion, nationality or political opinions; Substantial grounds to believe that if the request was granted, the person would be in danger of being subjected to torture; The granting of the request would prejudice the sovereignty, security, or national interest of the country, or other essential interests. The request concerns an offence for which the death penalty may be imposed in the foreign country (subject to exceptions). *Discretionary* grounds:	Required: English. *Problems* Variable quality of translations on incoming requests, which can delay the processing of the request (e.g. need for clarification by foreign authorities). *Solutions* Record is kept of efficient and skilled translators for outgoing requests. All MLA requests should be translated by translators who meet certain levels of proficiency in translating.

Country	Requirements (Q 2.1)	Grounds for refusal (Q 2.2)	Language of the request (Q 2.3)
		'Double criminality' principle is not respected; 'Ne bis in idem' and other: the request relates to a person who has been acquitted, pardoned, or has undergone punishment; Assistance could prejudice criminal investigations or proceedings in the requested country; Assistance could prejudice the safety of any person; Assistance would impose an excessive burden on the resources of the requested country; Any other situation where it is appropriate to refuse assistance.	
4. Austria	Compliance with the applicable procedure; Attachment, to the request, of the original or certified copy of the order from the relevant authority (in the absence of court order: statement by the foreign authority that conditions required under applicable law of the requesting country are satisfied).	Grounds depend on the factual background of the case and information required, and include a certain threshold of seriousness of the offence. E.g. A request for content data in a case of simple fraud will be refused.	Accepted: German, English, or French. Bilateral supplementary agreements may provide mutual waiver on translations. Suggestions: Advisable to waive the translation requirements (translation of better quality can be obtained in the requested State); Automatic translation programmes may have to be avoided.
5. Azerbaijan	Requirements set out by applicable international agreements, including the Convention on Cybercrime.	Execution of the request is incompatible with domestic law	Accepted: English, Turkish or Russian
6. Belgium	Legal cooperation is primarily governed by the Law of 9 December 2004. The MLA requests must be in conformity with	Only the grounds for refusal foreseen in the relevant instrument are applicable. However, the execution of a request can be delayed if this is in	Request received in English are accepted but must be translated into the three official languages of Belgium.

Country	Requirements (Q 2.1)	Grounds for refusal (Q 2.2)	Language of the request (Q 2.3)
	the international legal instrument on which it is based. The domestic legislation does not foresee additional requirements. Upon a request, - A prosecutor can obtain subscriber information from a provider without authorisation from an investigating judge (Art. 46bis Code d'instruction criminelle) - An investigating judge can obtain call or localisation data directly from a provider.	the interest of an ongoing investigation in Belgium.	Overall, the question is translations is a major challenge, given cost and also the limited number of qualified translators. A dynamic database or glossary with the key terms would be useful. Alternatively English could serve as common language for proceedings.
7. Bosnia and Herzegovina	*Content* of the request: name of the foreign authority, and if possible, the requested authority; legal basis; identification of the criminal offence and the suspect; factual description of the offence; damage involved; measures that should be taken; other relevant data. Compliance with the applicable procedure, in particular requirements for the issuance of a court order toward an ISP (suspicion of the commission of a criminal offence; the information can be used as evidence or any other way for criminal proceedings);	*Discretionary* grounds: - legal assistance may be refused on the basis of factual reciprocity in relation to a particular country. *Mandatory* grounds: a) if the execution of the request would prejudice the legal order of Bosnia and Herzegovina or its sovereignty or security; b) if the request concerns an offense which is considered to be a political offense or an offense connected with a political offense; c) if the request concerns a military criminal offense. d) if the person accused of the relevant criminal offense has been acquitted of charges based on the substantive-legal grounds or if the proceeding against him has been discontinued, or if he was relieved of punishment, or if the sanction has been executed or may not be executed under the law of the country where the verdict has been passed; e) if criminal proceedings are pending against the	Required: One of the languages of Bosnia-Herzegovina (i.e. Bosnian, Croatian, as well as Serbian), certified by a sworn translator. Tolerated: (Interpol channels) English. *Problems and solutions*: N/a.

Country	Requirements (Q 2.1)	Grounds for refusal (Q 2.2)	Language of the request (Q 2.3)
		person in Bosnia and Herzegovina for the same criminal offense, unless the execution of the request might lead to a decision releasing the accused from custody, f) if criminal prosecution or execution of a sanction pursuant to the national law would be barred by the statute of limitations *Practical issues*: Lack of elaboration of the request; impossibility to establish the criminal offence.	
8. Bulgaria	*Content* of the request: Information on the requesting authority; subject and reason for the request; name and nationality of the person concerned; name and address of the person to whom papers should be served; if necessary, charges and a summary of the relevant facts. Existence of a legal basis (international agreement, or in the absence of such agreement, based on the reciprocity principle)	Execution of the request may threaten the sovereignty, national security, public order and other interests protected by law. Execution of the request may hinder actions of investigation or gathering data for the initiation of criminal proceedings; Execution of the request may endanger a natural person's life; The data requested does not correspond to the objectives of the request; The data requested is related to a petty crime.	It depends on international agreements applicable between the requesting and requested countries. *Problems* Translation of requests takes too much time and money.
9. Costa Rica	Compliance with requirements established in the applicable international instruments. *Nota*. National authorities cooperate with the requesting State, with or without the support of an international agreement.	The request implies procedures or petitions opposites to fundamental rights and guarantees that the Political Constitution and the laws grant to the people.	Required: Spanish. *Problems* -Time required to translate requests; -Human and financial resources involved.
10. Croatia	*Form* of the request: Written form, or an electronic form leaving a written record, provided its authenticity can be established and the method of sending explained at request; *Content* of the request:	*Discretionary* grounds: The request concerns: a political offence or is connected to such an offence (international crimes excluded); a fiscal offence. Executing the request would prejudice the	Required: Croatian. Accepted: English ("if not possible in Croatian, English translation will be accepted"). Translations have to be officially

Country	Requirements (Q 2.1)	Grounds for refusal (Q 2.2)	Language of the request (Q 2.3)
	Place of issuance; name of the competent foreign authority sending the request; legal basis of the request; description and justification of the request; legal name, short factual and legal description of the offence*; information on the person concerned (data, nationality, position in the procedure); where relevant, type of court deed forwarded. *Exception: When the request relates to the service of court decisions and the like.	sovereignty, security, public order or other essentials interests of the State. Presumption that the person whose extradition is sought would be prosecuted or punished on grounds of race, religion, citizenship, affiliation with a specific social group, or political beliefs. The criminal offence is insignificant. *Mandatory* grounds: 'Ne bis in idem' and other: Cases of substantial acquittal in Croatia, discontinued procedure, relief from sentence, sanction has been executed or may not be executed under the applicable foreign law*. Criminal proceedings for the same offence are pending in Croatia (exception: execution of the MLA request may lead to the release of the accused). Criminal prosecution or sanction would be barred by the "Statute of limitations" under national law*. *Exception: The final judgment was revised in the requesting State.	certified. *Problems and solutions*: Translation, especially the time required for translating requests, undermines the efficacy of LEA action. Suggestion: MLA communications through contact points should be favoured.
11. Cyprus	A formal written request for assistance needs to be sent to the Central Authority i.e. the Ministry of Justice & Public Order it needs to include all elements for its execution (summary of facts, relevant law, and requested actions).	Grounds listed in Articles 25.4 and 27.4 Budapest Convention. Refusal if basic elements of a written request are not met. Prerequisite that the offence investigated in the requesting state to be punishable with imprisonment up to 5 years.	English and Greek language. Problems: Translations delay answers. Solution: use English.
12. Dominican Republic	Requests always need to be sent via the Public Ministry.	N/A	The request must be sent in Spanish.
13. Estonia	*Content* of the request: Name of the requesting authority; content [i.e.	The request may endanger the security, public order or other essential interests of the State;	Required: Estonian or English.

Country	Requirements (Q 2.1)	Grounds for refusal (Q 2.2)	Language of the request (Q 2.3)
	measures requested]; details of the person concerned; facts and legal assessment of the criminal offence.	The request conflicts with the general principles of national law; Reasons to believe that the request regards charges/punishment based on discriminatory grounds (race, nationality, religion, etc.); Nota. The political character of the offence is not a ground for denial in relation with EU countries (subject to exceptions)	*Problems* Additional work and extra costs entailed by the translation of all documents.
14. Finland	When coercive measures are needed, compliance with requirements of national law on this issue; *Form* of the request: In writing, as a recording, orally, or in electronic format; *Content* of the request: identification of the requesting authority, and if relevant, competent authorities for proceedings and investigations; object and reason for the request; information on the persons concerned; description of the offence and applicable law; the facts and criminal conduct; description of evidence sought and related information; allowances and expenses of witnesses or experts involved. Where the service of court document is requested, attachment of the document to be served; Form and content: Request can nevertheless be executed if problems regarding form and content are of such nature that they do not form an obstacle to execution.	*Mandatory grounds* Execution of the request would prejudice the sovereignty, security or other essential interests of the State; Execution of the request would be contrary to human rights principles, fundamental freedoms, or *ordre public*. *Discretionary grounds* The offence is a political offence or a purely military offence; The offender could no longer be prosecuted, under national law (lapse of time, pardon or other) Criminal investigations, prosecution or proceedings regarding the offence have been initiated in a State (Finland or third) with regard to the offence; Criminal investigations, prosecution or punishment or other sanction regarding the offence have been waived in a State (Finland or third) ; The offender has been sentenced or acquitted for the offence in a State (Finland or third); Execution of the request would impose an unreasonable burden on resources available.	Required: Finnish or Swedish Exceptions: Another language may be accepted, when authorised by Decree or more generally, when it is possible. *Problems and solutions* N/a.

Country	Requirements (Q 2.1)	Grounds for refusal (Q 2.2)	Language of the request (Q 2.3)
		Regardless of the provisions of the general MLA law, assistance will be provided as agreed in international conventions or other instruments. Thus, being a Party to the Convention on Cybercrime as such already creates obligations and responsibilities or defines grounds for refusal.	
15. France	Compliance with the applicable procedure under national law, including regarding the issuance of a judicial order.	The request aims at the direct transmission of data, for which national law requires the issuance of a judicial order; The request concerns a petty offence; Execution of the request is not justified enough, compared to the constraints it involves. As regards requests from EU countries (see art. 695-9-41 CPP), the execution of the request can only be denied if: -it would prejudice the fundamental interests of the State in matters of national security; -it would prejudice criminal investigations or endanger a person's safety; -it would be manifestly disproportionate or without object, with regard to the outcome referred to in the request.	Accepted: French and English. *Problems* As a requested State, no specific issues regarding requests translated by the national unit for Europol or Interpol. As a requesting State, translation cannot be done by certain staff lacking English skills. Suggestion: To favour English language trainings for staff dealing with international cooperation matters.
16. Georgia	*Content* of the request: Indication of the facts, legal qualification of the case, the purpose and necessity of the request; whenever possible, detailed description allowing identifying the person concerned. When the request requires search seizure: double criminality principle; the offence can be subject to extradition; compliance with other provisions of domestic law.	Execution of the request threatens sovereignty, public security, or other vital interests of the State; Execution of the request is incompatible with domestic law; The request relates to a political offence or related offence (subject to exceptions), or a purely military offence; Execution of the request endangers human rights and fundamental freedoms;	No specific requirements. In practice: Mainly English, French or Spanish. *Problems and solutions* Time required for translating requests. Suggestion: To favour the use of English and French.

Country	Requirements (Q 2.1)	Grounds for refusal (Q 2.2)	Language of the request (Q 2.3)
		Execution of the request violates the ne bis in idem' principle	
17. Germany	Issuance of the mutual assistance request by a judicial authority; Issuance of a judicial order or equivalent by the requesting State; Description of the facts in the request; Respect of the double criminality principle; Translation of the request.	The request does not comply with requirements under national law; Evidence is intended for proceedings for a crime punishable with capital punishment, without guarantees of the requesting State that such a penalty will not be imposed.	Required: German. *Problems* Time required by translations sometimes delays the execution of requests.
18. Hungary	Dual criminality is a condition for responding to a request.	Request - is against Hungarian law - threatens safety and public order of Hungary - concerns political or military crimes.	English. Main problem: time for translation. Requests should be sent to Hungary in English.
19. Iceland	Time limits: No specific time limits. However, according to Icelandic law, companies shall delete all stored computer/IP data within 6 months. Documentation: Description of the pending legal proceedings, information on the act involved, applicable provisions in the requesting state, information on what measures are requested, information on the individual/company the request concerns. Special requirements may be necessary when certain actions are sought. Double criminality: Yes. However, double criminality is only required regarding political offences when the request is from Denmark, Finland, Norway or Sweden.	Non-respect of the double criminality principle. The request concerns a political or military offence. Execution of the request is likely to prejudice the sovereignty, security or public order of the State. Reasonable grounds to believe that the proceedings are based on account of race, religion, nationality, political beliefs etc.	Icelandic, English, Norwegian, Danish or Swedish. As there are very few Icelandic translators outside Iceland it is usually better to receive requests in (good) English rather than (poor) Icelandic. The translations into Icelandic are generally very poor and sometimes impossible to understand!
20. Japan	Requirements set out by applicable	Grounds for refusal are based on the non-	Required: Japanese.

Country	Requirements (Q 2.1)	Grounds for refusal (Q 2.2)	Language of the request (Q 2.3)
	international agreements, including the Convention on Cybercrime. When the request is not based on treaty, the following requirements apply: Assurance of reciprocity; Double criminality principle; Non-political character of the offence; Demonstration in writing that the evidence is essential to the investigation (requests for the provision of evidence or testimony of witness).	compliance with following requirements: Assurance of reciprocity; Double criminality principle (unless provided otherwise by treaty); Non-political character of the offence; Demonstration in writing that the evidence is essential to the investigation (requests for the provision of evidence or testimony of witness). Additional grounds: Those provided for by any international agreement used as the legal basis.	*Problems* As a requesting State: Time required and limited number of capable translators with expertise.
21. Latvia	Decision of the competent domestic authority on the admissibility of the procedural action to execute the request; (Pre-trial) Consent by the competent authorities (Prosecutor General's Office; State Police) to execute the request; Attachment of sufficient information and of the required documentation (e.g. a court order for disclosure of content data).	The request concerns a political offence (exceptions: terrorism, financing of terrorism); Execution of the request may harm the sovereignty, security, social order or other substantial interests of the State; Lack of sufficient information, without the possibility to obtain additional information.	Required: Latvian (except when agreed otherwise with the requesting State). Problems: Time needed for translating requests.
22. Lithuania	(See article 29 of the Budapest Convention) Content of the request: Identification of the requesting authority, the offence concerned, a brief summary of facts, the data to be preserved and its relationship with the offence, information identifying the custodian of the data or the location of the computer system, the necessity of the preservation, the intention to submit a mutual assistance request for search, seizure, disclosure and related actions. No grounds for refusal.	Lack of information provided for in article 29 of the Budapest Convention or the information provided is evidently inaccurate and no additional information is obtained; Contradiction to the legal principles of the national (Constitutional) law or international law (non bis in idem, non-discrimination, impartiality, fair trial, etc.); There is reasonable ground to believe that execution of the request is likely to prejudice the essential interests of the State (sovereignity, security, public order, human life, etc.);	Preferred languages: Lithuanian, English or Russian. *Problems* No major problems as regards requests translated in English or Russian. Other languages require extra time and money.

Country	Requirements (Q 2.1)	Grounds for refusal (Q 2.2)	Language of the request (Q 2.3)
		There is reasonable ground to believe that at the time of disclosure the offence, on which the request is based, is not considered as a crime by the laws of the Republic of Lithuania.	
23. Moldova	*Form* of the request: In writing; *Content* of the request: Identification of the authority addressing the request; name and address (if available) of the receiving authority; international legal basis of the request; description of the criminal case, including facts, relevant provisions in the Moldovan Criminal Code, damage caused; details of the person making the request; claim and data necessary to carry them, including circumstances, list of documents, evidence requested, etc.; expected date for a reply; attachment of all procedural acts needed; signature and official stamp of the requesting authority.	*Discretionary* grounds: The request concerns a political offence (exception: international crimes under the Statute of the ICC), or a purely military offence; Execution of the request is likely to prejudice the sovereignty, security or public order of the State; Reasonable rounds to believe that the proceedings are based on account of race, religion, nationality, political beliefs, etc.; The person will not have access to a fair trial; The requesting State punished the offence by the death penalty and gives no guarantee of its non-application or non-performance; Non-compliance with double criminality principle; or absence of criminal liability under domestic law.	Required: Moldovan. Tolerated: English. Note: Moldovan or other languages (according to applicable international agreements). *Problems and solutions*: Financial burden and time required for translating requests (especially for native languages). Suggestion: Favour English in MLA communications.
24. Montenegro	*Content* of the request: Name and seat of the authority sending the request; name of the requested authority, or as a minimum indication of the country and competent judicial authority; legal basis of the request; form and justification of assistance requested; legal qualification of the offence and summary of the facts*; where relevant, type of court writ forwarded. *Exception: When the request relates to the	[to be clarified]	Required: The official language. Tolerated: Official languages of the Council of Europe (English, French). *Problems and solutions*: No specific problems, since requests are usually translated into English.

Country	Requirements (Q 2.1)	Grounds for refusal (Q 2.2)	Language of the request (Q 2.3)
	service of court decisions and the like.		
25. Netherlands	Existence of a criminal case (i.e. initiation of foreign criminal proceedings); The conduct amounts to an offence according to the law of the requesting State; The conduct amounts to an offence according to domestic law; The offence is listed in offences for which pre-trial detention is allowed.	*Mandatory* grounds The request relates to a conduct being prosecuted at the domestic level; Non-compliance with the double criminality principle; Grounds *subject to a waiver* by the MoJ: The request raises fear of a discriminatory prosecution; The request relates to a political offence; or a tax offence; Instructions were given by the MoJ not to execute the request.	(Only applicable to requests based on the UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances). Required: Dutch, French, English or German. *Problems* N/a.
26. Norway	Double criminality principle; (Practical requirement) Identification of the legal/moral person holding the data; Regarding IP logs, respect of the time limit currently applicable (21 days).	Non-respect of the double criminality principle; The request regards defamation, and does not provide enough clarification about the alleged crime; Execution of the request would create practical difficulties (e.g. too many witnesses to interview).	Favoured: English, Norwegian, Swedish or Danish. *Problems* Limited capacity of in-house translators; Necessity, as a requested State, to translate the main documents and facts in Norwegian.
27. Philippines	The Department of Justice handles all communications relative to mutual assistance. *As requested State:* evaluation execution of request either through DOJ or other competent authorities upon execution, documents/evidence requested forwarded to DOJ	The grounds for refusal are different from one Bilateral Agreement on MLA to another. E.g. the MLA agreement with India provides the grounds for a party to refuse assistance as follows: a. The execution of the request would impair its sovereignty, security, public order or other essential interests, or prejudice the safety of any person; b. The execution of the request would be	The use of English as an internationally accepted language is practical and convenient for the parties.

Country	Requirements (Q 2.1)	Grounds for refusal (Q 2.2)	Language of the request (Q 2.3)
	DOJ transmits the documents/evidence requested to CA of the requested State on the basis of reciprocity: (G.R.: request is granted if the requesting State guarantees reciprocity) no compulsory measures, request may be executed upon execution, documents/evidence sought transmitted to the requesting State through diplomatic channels *As Requesting State:* law enforcement/prosecution authorities submit request to the DOJ evaluation in case of insufficient information, coordinate with the requesting agency/authority for completion/compliance with the requirements where request is urgent, DOJ informs CA of the requested State of the forthcoming request upon completion of the requirements, DOJ transmits request to CA of the requested State	contrary to the domestic law of the Requested Party; c. If the request seeking restraint, forfeiture or confiscation of proceeds or instruments of activity which, had it occurred within the jurisdiction or the Requested Party, would not have been an activity in respect of which a confiscation order could have been made; and d. The request relates to an offense in respect of which the accused person had been finally acquitted or pardoned. As a requesting State: Complexity of the system As a requested State: Restrictive laws and different jurisprudential interpretation by the court.	
28. Portugal	Compliance with requirements set for the search, seizure and disclosure of data under national law, including the issuance of an order from the competent judicial authority (except when provided otherwise).	*Mandatory* grounds: The proceedings do not comply with the ECHR; The request raises concerns of discrimination (on account of a person's race, religion, sex, nationality, language, political beliefs, etc.); The request involves proceedings before a court of exceptional jurisdiction or the enforcement of a sentence in such context; - The offence is punishable by the death penalty, or an irreversible injury of the person's integrity;	Required: Portuguese (except where provided otherwise in an international agreement). *Problems* Serious concerns raised by: -The time and money involved; -The difficulty to find skilled translators, especially for uncommon languages.

Country	Requirements (Q 2.1)	Grounds for refusal (Q 2.2)	Language of the request (Q 2.3)
		The offence is punishable by a life-long or indefinite sentence; The request regards a political offence, or a purely military offence.	
29. Romania	*Content* of the request: Name of the requesting and requested judicial authority; object and reasons of the request; legal classification of acts; information to identify the person concerned (accused, defendant, witness, expert, etc.); supporting documents, certified by the requesting authority; Compliance with the requirements for direct transmission, where applicable, or for other modalities of transmission; Reference to the legal basis (international agreement), or a written assurance of reciprocity from the competent authority of the requesting State (subject to exceptions).	Execution would prejudice the State's sovereignty, security, public order and others, as defined by the Constitution; Criminal prosecution has taken place for the same act and (a) a final judgement stated the acquittal or ceasing of the criminal trial; or (b) the penalty imposed through a final sentence has been served or was subject to a pardon or amnesty. (Exceptions: The request purports to review the final decision – under conditions set out by national law – or an applicable treaty sets out more favourable conditions as regards the principle of 'ne bis in idem'). Grounds applicable in extradition cases.	Accepted: Romanian, English or French. *Problems* Financial resources needed to translate the numerous requests and documents attached; Poor quality of translation, requiring a new translation and hence additional time and costs.
30. Serbia	*Content* of the request: Legal basis; description of actions in relation to the request; justification of the request; any other relevant data. Compliance with the applicable procedure, in particular requirements for the issuance of a court order (compulsory for interception or collection requests). 'Double-criminality' principle (the offence is criminalised under national law). Criminal proceedings under national law have not been fully completed.	Grounds set out in the Cybercrime Convention. Grounds set out under national law: *(Non-compliance with any of the requirements detailed in Q 2.1, see left column)*	Required: Serbian. Tolerated: English. *Problems and solutions*: Financial burden and time required for translating requests. Suggestion: English should be favoured in MLA communications.

Country	Requirements (Q 2.1)	Grounds for refusal (Q 2.2)	Language of the request (Q 2.3)
	Criminal prosecution is not excluded due to the status of limitations, amnesty or pardon. The request does not refer to a political offence or a related offence; military offences. The request would not prejudice sovereignty, security, public order or other essential interests of the State.		
31. Slovakia	The MLA request has to be sent by a competent authority of the requested state with a proper translation into Slovak (in case of non-treaty based cooperation) or any other language (depending on the language regime regulated in a given treaty). A content of request must be sufficient for the execution of such request. It should include, in particular, a reference to an international treaty (if there is treaty bases), a description of the offence, including date, place of the offence, personal details of persons involved, legal qualification, applicable provisions of the laws of requesting state (in order to enable the judicial authority to evaluate dual criminality, where applicable), links to Slovakia, clear description of the action expected from the Slovak authorities (it is extremely important to enter into communication with competent authorities from the moment, when a request under Article 29 is delivered to the requested state).	Ground listed in Articles 25.4 and 27.4 Budapest Convention.	Language requirements depend on the applicable international treaty. If there is no treaty based cooperation, a translation into the official language (Slovak) is required. The use of English seems to facilitate the cooperation. Some countries provide for translation into Slovak. So far no difficulties occurred in relation to the translation issue. It may be helpful, in particular in urgent cases, to introduce a new provision in the (possible) Second Additional Protocol, on the obligation to accept request under Article 29 in English in urgent cases. The same obligation may be considered for MLA requests (in urgent cases only).
32. Slovenia	Description of the grounds to suspect the commission of an offence; Compliance with requirements for the issuance	No experience in this matter. Existing grounds:	Accepted: English. (Domestic authorities translate requests to Slovenian).

Country	Requirements (Q 2.1)	Grounds for refusal (Q 2.2)	Language of the request (Q 2.3)
	of a judicial order, where applicable; Form of the request: Written form; Content of the request: Information allowing to identify the means of electronic communications; inducement of reasonable grounds; time period for which the data is required; other circumstances justifying the execution of the request	The data requested is related to national security; The request concerns a case for which proceedings have already been initiated.	
33. Spain	Usual legal requirements for mutual assistance requests: translation, description of facts, description of the offence, etc.; Issuance of a judicial order to obtain the data from ISPs and other holders of data; The request must relate to a serious crime.	No information available.	Required: Spanish. (Subject to exceptions provided by bilateral agreements). *Problems* Time and money involved; Lack of practitioners having skills in foreign language.
34. Switzerland	Request from a judicial law enforcement authority; Sufficient presentation of the facts (modus operandi); Translation of the request (German, French, Italian); Compliance with the applicable procedure, including the issuance of a court order; The offence must be punishable in both requesting and requested States; The measures required are proportionate to the objectives set in the request.	Absence of translation in an accepted language; No competence of the requesting authority to request mutual assistance; The request is retroactive and regards data stored for more than six months; Lack of information of the facts (modus operandi)	Required: German, French, or Italian. In practice, a draft in English can be presented to national authorities.
35. "The former Yugoslav	*Form* of the request: MLA letter Content of the request: Type and location of	The request concerns a political offence or a related offence, or a fiscal offence.	Required: No specific requirement (national language of the requesting

Country	Requirements (Q 2.1)	Grounds for refusal (Q 2.2)	Language of the request (Q 2.3)
Republic of Macedonia"	data requested; criminal offence involved; legal basis (Criminal Code). Compliance with the applicable procedure, including issuance of a court order	The execution of the request is likely to prejudice the sovereignty, security, ordre public or other essential interests of the State.	authority is accepted). The MoJ translates requests into Macedonian. *Problems and solutions*: Costs of translation. Suggestion: Harmonisation of MLA procedures by type, content and language.
36. Turkey	Precondition: Existence of an international agreement, or respect of the reciprocity principle. Content of the request: identification of the requesting authority; object and justification of the request; type and location of the data; identity and nationality of the person concerned (where available); relation between the data sought and a type of crime; legal basis (Criminal Code); description of the facts, criminal offence and penalties involved.	Grounds set out in applicable international instruments. Inability of foreign authorities to give guarantees, in case where a seizure or confiscation requested may lead the financial damage. Absence of proportionality of the request. Lack of grounds to execute the request.	Required: Turkish. Tolerated (urgent cases): English. *Problems and solutions* Suggestion: Harmonisation of MLA requests in English and national language.
37. Ukraine	(MoI) Main requirement: Approval of the General Prosecutor's Office, with or in the absence of an MLA agreement. E.g. 2012, approval and execution of a request from Japan. (Sec Serv) -Compliance with the Cybercrime Convention [where applicable], and international law;	(MoI) Any ground provided for by an applicable international agreement. In the absence of such agreement, the following grounds apply: The request contradicts the Constitution, and can harm the sovereignty, security, public order, or other interests of the State; 'Ne bis in idem': the person concerned has already been judged and the decision came to effect; No support given to mutual assistance by the	(MoI) Required: As set forth in the applicable international instrument. *Problems*: N/a (no competence). (Sec Serv): As set forth in international agreements, or in the language of the country obtaining the request or in

Country	Requirements (Q 2.1)	Grounds for refusal (Q 2.2)	Language of the request (Q 2.3)
	Compliance with the procedure under national law.	requesting State when needed; The request relates to a petty crime, not punishable under domestic law; Grounds to think that the request pursues discriminatory objectives, based on race, skin colour, political opinion, religion, sex, etc. The offence is subject to ongoing pre-trial investigations or trial. (Sec Serv): See above.	English. *Problems* Translation is rendered difficult by the use of specific terms and language in judicial documents.
38. United Kingdom	*Content* of the request: Information on the source of telephone numbers; exact data, time and place of the incident investigated; details and role of individuals involved; reasons and objectives of the request; reasons as to why such objectives cannot be achieved by other means; relevant information for consideration of a possible intrusion into the privacy of third parties and plans to minimise this. Where interception of communication is sought, the requesting State must be an EU Member State.	Request not complying with domestic legislative requirements; Execution of the request is not possible on policy grounds (e.g. the request is politically motivated).	Required: English. *Problems and solutions* Sending of all requests should be in English.
39. United States of America	Issuance of a (domestic) court order: (a) a production order, when non-content information is sought and the provider is not willing to provide it voluntarily; (b) a search warrant, when content information is sought. Conditions: double criminality (infrequently); 'probable cause' principle — i.e.	Any of the grounds set out by the Convention on Cybercrime; The information provided is not sufficient to meet the domestic quantum of proof to obtain data; The conduct is not a criminal offence under domestic law; The request contradicts essential interests of the	Required: English. Non-formal requests may be transmitted in the original language. *Problems* Time and money required to complete translations;

Country	Requirements (Q 2.1)	Grounds for refusal (Q 2.2)	Language of the request (Q 2.3)
	the information provides a reasonable basis to believe that a crime has been committed and that the account concerned contains evidence of that crime). Information showing the relation between the data sought and the case investigated;	State (especially in matters of free expression).	Poor quality of certain translations, causing delays in processing requests.

3.6.2 Legal basis

Country	Legal basis (Q 2.1.2)
1. Albania	Cybercrime Convention; CoE's European Convention on Mutual Assistance in Criminal Matters Law On Jurisdictional Relations with Foreign Authorities in Criminal Matters of Republic of Albania
2. Armenia	Regulated by Article 499' 6 of CPC of RA.
3. Australia	*Mutual Assistance in Criminal Matters Act 1987*, including section 15B; *Telecommunications (Interception and Access) Act 1979,* sections 110, 116 and 117.
4. Austria	International agreements, where applicable; *Austrian Federal Law on Extradition and Mutual Legal Assistance*, including section 56 § 2;
5. Belgium	Law of 9 December 2009.
6. Bosnia and Herzegovina	Cybercrime Convention; CoE's European Convention on Mutual Assistance in Criminal Matters. Law on Mutual Legal Assistance in Criminal Matters (The Official Gazette of Bosnia and Herzegovina, no. 53/09, 58/13), articles 1-8. Criminal Procedure Code of Federation of Bosnia and Herzegovina; Criminal Procedure Code of Republika Srpska; Criminal Procedure Code of Brcko District
7. Bulgaria	*Criminal Procedure Code*, including article 471
8. Costa Rica	*Public Ministry's Statutory Law*; *Penal Procedural Code*
9. Croatia	Cybercrime Convention;

Country	Legal basis (Q 2.1.2)
	CoE's European Convention on Mutual Assistance in Criminal Matters. Act on International Legal Assistance in Criminal Matters (Official Gazette 178/04)
10. Cyprus	The legal basis for the execution of a request is the Cybercrime Ratification Law of 2004, and the national law on International Cooperation in Criminal Matters.
11. Dominican Republic	*International and bilateral agreements.*
12. Estonia	*Criminal Procedure Code*, articles 462-463.
13. Finland	*Act on International Legal Assistance in Criminal Matters* (4/1994) International agreements, where applicable.
14. France	*Code de procedure pénale*, article 695-9-31 to 695-9-47 and aarticle R49-35 to R49-39.
15. Georgia	*Law "On International Cooperation in Criminal Matters"*, article 2.
16. Germany	*Section 59 of the Act on International Legal Assistance in Criminal Matters*, in conjunction with international agreements and/or the *Code of Criminal Procedure*, sections 94-100.
17. Hungary	International assistance in criminal matters Act of 1996. Act XXXVIII. Act 61-75. § Other agreements.
18. Iceland	Act on extradition of criminals and other assistance in criminal proceedings, No. 13/1984. English translation: http://eng.innanrikisraduneyti.is/laws-and-regulations/english/extradition-and-other-assistance/
19. Italy	N/a.
20. Japan	*Act on International Assistance in Investigation and Other Related Matters*, including article 8
21. Latvia	*Cybercrime Convention;* CoE's European Convention on Mutual Assistance in Criminal Matters; *Criminal procedure law*, article 845
22. Lithuania	*Law No. IX-1974, 22 January 2004 on the Ratification of the Cybercrime Convention* (published in Official Gazette No. 36-1178, 2004); *Code of Criminal Procedure*.
23. Moldova	*Criminal Procedure Code of the Republic of Moldova*, article 536.
24. Montenegro	Cybercrime Convention; CoE's European Convention on Mutual Assistance in Criminal Matters. Law on Mutual Legal Assistance in Criminal Matters (Official Gazette of Montenegro, No. 04/08, 17 January 2008)
25. Netherlands	*Code of Criminal Procedure*, title X; International agreements, where applicable.

Country	Legal basis (Q 2.1.2)
26. Norway	*Criminal Procedure Act* article 215a; *Courts of Justice Act*, article 46
27. Philippines	The legal basis in executing request for mutual assistance is primarily the Bilateral Agreement between the Philippines and a particular country on mutual legal assistance in criminal matters. Hence, the legal basis would differ from one agreement to another. Currently, the Philippines has MLATs with the United Kingdom, Australia, United States, Hong Kong, Switzerland, Republic of Korea India and Spain.
28. Portugal	*Law on Cybercrime*, articles 24 and 15
29. Romania	*Law no. 302/2004 on International Judicial Cooperation in Criminal Matters (republished);* *Criminal Code and Criminal Procedure Code* *Law No. 161/2003 Title III (The Prevention and Countering of Cybercrime);* *Law no. 508/ 2004 on the Creation, Organization and Operation of the Directorate for Investigating Organized Crime and Terrorism;* *Law 39/2003 on the Prevention and Combating of Organized Crime;* *Law 656/2002 on the Prevention and Sanctioning of Money Laundering* *Bileteral and multilatereal agreements, in particular Cybercrime Convention*
30. Serbia	Cybercrime Convention; CoE's European Convention on Mutual Assistance in Criminal Matters. Law On Mutual Assistance In Criminal Matters of the Republic of Serbia
31. Slovakia	Legal basis: The provisions of Articles 537,538,539 of the Code of Criminal Procedure are combined with Articles 90, 115,166 of the Code of Criminal Procedure, as applicable.
32. Slovenia	*Criminal Procedure Code*, including articles 148, 149b, 164, 220 and 515
33. Spain	*Law 25/2007* (transposing the Directive 2006/24CE) and other (law on judges, law on prosecutors and *Criminal Procedure Code*); Applicable international agreements.
34. Switzerland	*Federal Act on International Mutual Assistance in Criminal Matters* (Mutual Assistance Act, IMAC) of 20 March 1981.
35. "The former Yugoslav Republic of Macedonia"	United Nations Convention against Transnational Organized Crime; Cybercrime Convention. Code of Criminal Procedure, chapter XXX.
36. Turkey	Bilateral agreements; United Nations multilateral conventions; OECD conventions; CoE's European Convention on Mutual Assistance in Criminal Matters.

Country	Legal basis (Q 2.1.2)
	No specific legislation on mutual assistance (in preparation). Existence of a circular of the MoJ to implement MLA requests.
37. Ukraine	(MoI) *Criminal Procedure Code*, articles 554-572. (Sec Serv) *Criminal Procedure Code*, part IX (article 543).
38. United Kingdom	*The Crime (International Co-operation) Act* 2003 (CICA); Applicable international agreements.
39. United States of America	Title 18, *U.S.C.*, Section 3512.

3.6.3 Procedures (Question 2.4) and problems encountered (Question 2.5)

2.4 Procedure: step by step procedure for sending/receiving and follow up to requests As a requested State: Please describe step-by-step the complete procedure that you follow when receiving a request for stored computer data. As a requesting State: Please describe step-by-step the complete procedure that you follow when sending a request for stored computer data. 2.5 The main problems encountered with regard to mutual assistance regarding accessing of stored data Which are the main problems for you as a requesting State? Please elaborate and provide examples. Which are the main problems for you as a requested State? Please elaborate and provide examples.

Country	Procedure for sending/receiving requests (Q 2.4)	Problems encountered (Q 2.5)
1. Albania	As a *requesting* State: Request for the obtaining of data from the data holder (ISP or other legal person) with the assistance of the LEA. The foreign LEA contact point is immediately contacted. In the meantime, a formal rogatory letter is sent to foreign authorities. As a *requested* State: Upon reception, transmission of the request by the Ministry of Justice to the competent court; The court decides to transmit the request to the prosecution; The prosecution executes the request through the LEA, ISP or other private entities; The obtained data is transmitted to the foreign judicial authority.	As a *requesting* State: Time issues (duration of the procedure; tight deadlines to handle evidence). Discrepancies between legal systems. As a *requested* State: Legal restrictions based on the protection of personal data; Time issues (duration of the procedure; tight deadlines to handle evidence). Discrepancies between legal systems.
2. Armenia	The General Prosecutor's Office is responsible for receiving MLA requests.	As requesting State: Foreign countries refuse cooperation without MLA request. MLA requests require a criminal case. However, criminal cases cannot be initiated without

Country	Procedure for sending/receiving requests (Q 2.4)	Problems encountered (Q 2.5)
		sufficient information and evidence first. As a requested State: A court order is required within Armenia to obtain the data. This can take time and is sometimes denied.
3. Australia	As a *requesting* State: 1° Possibly, informal enquiries of the foreign country to determine whether it is possible to obtain stored computer data and the legal thresholds to be met. Australia determines whether it is possible to preserve that data pending a formal MLA request; 2° Australian LEA seeks preservation of the stored computer data; 3° The Attorney-General's Department liaises with LEA or prosecution agency which is seeking the stored computer data to ensure there is sufficient information to include in a formal request to that foreign country to meet the foreign legal thresholds; 4° The Attorney-Genera 's Department l sends a formal mutual assistance request to the foreign country seeking the stored computer data; 5° The Attorney-General 's Department liaises with the foreign country regarding provision of the stored computer data. As a *requested* State: 1° Request by the foreign country; 2° Attorney-General's authorisation; 3° Application by Australia police officer to the competent judicial authority to obtain a warrant over the stored computer data; 4° The judicial authority considers the application for a warrant and may issue a warrant;	As a *requesting* State: Making sure that the request meets the foreign country's legal thresholds for providing stored data (Possible solution: Direct contact, where possible, with foreign central authorities for advice on how to meet the thresholds); Ensuring that material is preserved and not deleted prior to the formal request being made and the warrants executed to obtain that material; Time involved in obtaining stored data from foreign countries (often a minimum of 6-12 months). As a *requested* State: Lack of sufficient information in the request, leads to a time and resource intensive process to seek additional information; it may also preclude national authorities from verifying that thresholds are met, and the authorisation or warrant may thus not be obtained.

Country	Procedure for sending/receiving requests (Q 2.4)	Problems encountered (Q 2.5)
	5° Access to stored communications; 6° Provision of material to foreign country.	
4. Austria	As a *requesting* State: 1° Preparation of the request by the competent prosecutor (including translation and "legalisation" of documents); 2° Forwarding of the request either directly or through the central authority (via diplomatic channels in the absence of international agreement). As a *requested* State: 1° Reception of the request either directly by the executing authority or by the Federal Ministry of Justice (depending on international agreements); 2° Following legal verifications, forwarding of the request by the MoJ to the locally competent prosecution service for its execution; 3° Where applicable, issuance of an order by the prosecutor with the approval of the court; 4° Execution of the order by the police under the supervision of the prosecution service. 5° Transmission of the results to the requesting State either directly or through the central authority.	As a *requesting* State: Refusal of requests related to petty offences; Lack of knowledge of time limit of storage of data prescribed by law. As a *requested* State: Lack of documentation required under national law (see Q 2.1.1) Lack of clarity of the request (type of data; period of time for the production of the data).
5. Azerbaijan	As a requested State: The central authority receives the request; The central authority is requesting court decision to obtain data the central authority is obtaining data from ISP's (and etc.) after court decision, After internal procedures, the central authority is sending the data to the requesting state	
6. Belgium	As a requesting State: See below modus modendi.	Delays in the response time.

Country	Procedure for sending/receiving requests (Q 2.4)	Problems encountered (Q 2.5)
	As a requested State: The request is received directly by a foreign judicial authority. If sent to the central authority (in Belgium the Federal Prosecution Service), that one forwards the request to the competent territorial judicial authority. If it concerns several authorities or if it is unclear which one is responsible, the Federal Prosecution Service executes or coordinates the execution. An investigating judge is only involved if coercive measures are required, such as for obtaining stored computer data.	Obtaining data depends on the internal policies of enterprises. Some require an MLA request while others are able to provide traffic data directly to a prosecution service. Obtaining content data requires a certain level of proof which is not possible unless the data are actually obtained (vicious circle).
7. Bosnia and Herzegovina	As a *requesting* State: Transmission of the request through the Ministry of Justice; (Exception, provided by treaty: Direct transmission by national judicial authorities to their foreign counterparts; use of Interpol channels, use of Eurojust) As a *requested* State: Transmission of the request, through the Ministry of Justice, to the competent judicial authority (Exception: Direct transmission through Interpol in urgent cases). In the absence of, or when envisaged by, a treaty, the Ministry of Justice transmits/receives requests through the Ministry of Foreign Affairs. The police inform the prosecutor on all relevant facts, and request his/her approval. Following approval, the competent court issues an order to the telecom operator (e.g. for the delivery of data by an ISP). The police then implement the court order.	As a *requesting* State: Lack of awareness of the person to be contacted in case of emergency (e.g. to secure data until the transmission of an official MLA request). As a *requested* State: N/a.
8. Bulgaria	As a *requesting* State: The request shall be forwarded to the	As a *requesting* State: Delay or failure in the execution of requests by

Country	Procedure for sending/receiving requests (Q 2.4)	Problems encountered (Q 2.5)
	Ministry of Justice (except where an international agreement provides for a different procedure). As a *requested* State: N/a. [to be clarified]	authorities of some countries. As a *requested* State: No specific problems.
9. Costa Rica	As a *requesting* State: 1° Coordination of the preparation of the request by the competent Prosecutor and the Office of Technical Consultancy and International Relations (OATRI) (form of evidence required; type of offence; facts; emergency level, etc.); 2° Identification by the OATRI of the applicable cooperation instrument and the competent central authority to process it; 3° (a) If the central authority is the OATRI, the request is directly sent to the competent central authority in the requested State; 3° (b) If the central authority is another institution, the request is transmitted to the latter, which in turn sends it to the central authority in the requested State; 4° Once the request is executed and a response received, the OATRI verifies that it followed the applicable channels and forwards the response to the competent Prosecutor. As a *requested* State: 1° The OATRI receives the request (directly when it is the central authority, or indirectly through the competent central authority); 2° Review by the OATRI of the compliance of the request with requirements of applicable instruments or national law, and addresses other issues (e.g. questions for witnesses); 3° Identification by the OATRI of the competent authority for the execution of the request (prosecutor, OATRI itself, etc.); 4° Verification by the OATRI that the execution is in accordance with what was requested and with national law, and sending of the requests through the central authority or other appropriate	As a *requesting* State: In one particular situation, a request for data about a user account of a social network in the USA was denied on the ground that it did not reach a priority threshold. As a *requested* State: N/a.

Country	Procedure for sending/receiving requests (Q 2.4)	Problems encountered (Q 2.5)
	channel (e.g. diplomatic channel).	
10. Croatia	As a *requesting* State: The competent court transmits a formal request [to the Ministry of Justice]; The Ministry of Justice sends an official request to the requested State; Upon reception of a reply, the Ministry of Justice forwards it to the court which initiated the request. As a *requested* State: Upon reception by the Ministry of Justice, transmission of the request to the competent court; Once the court has executed the request, a response is sent to the requesting State.	As a *requesting* State: Time required before a reply is given to the request. As a *requested* State: N/a.
11. Cyprus	As a requested State: 1. As soon as a request is received, police will apply to court for an order to obtain stored data. 2. Apply to ISP to obtain information on owner of computer 3. Apply to court for warrant to search house/computer of the suspect. As a requesting State: Following an investigation, an MLA request is sent via the Ministry of Justice and Public Order.	As a requested States: Overloaded by requests. As a requesting State: Time consuming in order to prepare all relevant documents and the procedure for sending the MLA, as well as the time for receiving answer to the request.
12. Dominican Republic		The requested information is usually not received on time.
13. Estonia	As a *requesting* State: ["Please see above". [to be clarified]]. As a *requested* State: 1° Following verification of legal requirements by the Ministry of Justice, transmission of the request to the Public Prosecutor's	As a *requesting* State: No preservation of the data in the requested State, even in certain Parties to the Cybercrime Convention; Difficulty of cooperation with non-EU States (absence of reply). As a *requested* State:

Country	Procedure for sending/receiving requests (Q 2.4)	Problems encountered (Q 2.5)
	Office (PPO); 2° Following verification by the PPO of the admissibility and feasibility of measures required by the request, transmission to the competent judicial authority for its execution(*); 3° Sending of materials obtained to the MoJ via the PPO; 4° Forwarding of the materials by the MoJ to the requesting State (or via Eurojust, for requests sent through this channel) (*)In urgent cases: requests submitted via Interpol channels or a Schengen notice can be executed with the approval of the PPO, before a formal MLA request is received by the MoJ.	No problem, especially since requests for IP addresses are not considered as surveillance activity anymore.
14. Finland	*As a requesting* State: 1° Preparation of the request by the National Bureau of Investigation (NBI) or a local police department; 2° Transmission of the request to the NBI for quality control and translation into foreign language; 3° Sending of the request (a) (non-EU countries) from the Ministry of Justice, or (b) (EU countries) directly from the NBI to the requested State. In EU of European Evidence Warrant (EEW) cases a prosecutor in most cases issues the EEW. Generally the prosecutor has an essential role in evaluating whether and for which issues MLA will be requested. Police and prosecution authorities have an obligation to cooperate during criminal investigations. As a *requested* State: 1° Reception of the request by: (a) (non-EU countries) the Ministry of Justice, or directly to the competent authorities; the request is then sent to the NBI; or (b) (EU Member States) directly the NBI. 2° Verification of legal requirements by the NBI;	As a *requesting* State: Time required when the request are sent via Ministries of Justice' channels; Time required to obtain replies from specific countries. As a *requested* State: Requests made on a weak basis, indicating the lack of quality control in the requesting State. Non-compliance with all legal requirements applicable.

Country	Procedure for sending/receiving requests (Q 2.4)	Problems encountered (Q 2.5)
	3° Execution of the request by the NBI or a local police department, including via coercive measures if needed and legally possible; 4° Compilation of evidence by the NBI; 5° Sending of documents (a) (non-EU countries) to the Ministry of justice, to be then forwarded to the requesting State; or (b) (EU countries) directly to the requesting State.	
15. France	[to be clarified] As a *requesting* State: Since 2012, any request transmitted via Interpol channels passes by the National Unit, which forwards it to the requested foreign National Bureau. As a *requested* State: 1° The request received through Interpol channels is registered in an international mail database within the Directorate; 2° The request is handled by the operational documentation section.	As a *requesting* State: Difficulty to obtain personal data without a letter rogatory. As a *requested* State: Impossibility for the national police to transmit personal data requiring the issuance of a judicial order — even when for simple requests for IP addresses; Workload implied by letters rogatory for such basic information; Requests concerning isolated case or a limited prejudice (e.g. Request for any information regarding a credit-card fraud, for which the prejudice was 750€).
16. Georgia	As a *requesting* State: 1° Transmission of the request by the relevant LEA to the Ministry of Justice; 2° Verification of legal requirements by the Ministry of Justice; 3° Sending of the request by (a) (trial stage) the Ministry of Justice itself, or (b) (during criminal intelligence gathering) by its subdivision, the General Prosecutor's Office. In parallel, information is provided to the requested State as to the time limit preferred for executing the request. As a *requested* State:	As a *requesting* State: Protracted procedure of mutual assistance (e.g. to identify the competent authority for the provision of the information needed). As a *requested* State: Technical obstacles encountered (e.g. difficulty of domestic ISPs to store access and server logs for a sufficient period). Nota. Lack of practice.

Country	Procedure for sending/receiving requests (Q 2.4)	Problems encountered (Q 2.5)
	1° Translation of the request; 2° Verification by the LEA of formal requirements and potential grounds for denial; 3° Transmission of the request to the most relevant internal organ for further response, and provision of information to the requesting State as to the time required for execution; 4° Sending of the response, including information and documentation, to the requesting State via diplomatic or other direct channels.	
17. Germany	As a *requesting* State: 1° Examination as to whether the data has been provisionally preserved, and if it has not, recommendation to do so; 2° Verification of the compliance of the request with legal requirements of the requested State; 3° Sending of the request, together with its translation, to the requested State. As a *requested* State: 1° Preliminary contact by the 24/7 contact point with the competent prosecutor on the possible initiation of domestic investigations; 2° The data can already be secured upon issuance of an order by (a) a court; or (b) the police or prosecutor (in exigent circumstances and if traffic data is not concerned); 3° Official reception of the mutual assistance request 4° Verification of legal requirements by the Federal Office of Justice, and that data has been preserved provisionally; 5° Forwarding of the request to the competent Land judicial authority; 6° Transmission of the seized data to the requesting State.	As a *requesting* State: High standard imposed for the statement of facts, requiring the gathering of additional information and delaying the execution of the request; Time needed for the execution of requests related to subscriber data As a *requested* State: No problems have been reported so far.

Country	Procedure for sending/receiving requests (Q 2.4)	Problems encountered (Q 2.5)
18. Hungary	As a *requested* State: Receive the request => Translation => Send the request to the competent operator => Receive the answer => Translation => Send the answer to the requesting country As a requesting State: The Hungarian investigation authority sends the request to the Hungarian International Law Enforcement Cooperation Centre => Translation => Send the request to the international law enforcement cooperation centre of the concerned country => Receive the answer => Translation => Send the answer to the requesting authority.	As a requesting State: A rogatory letter is necessary to get the call list. As a *requested* State: Mostly a rogatory letter is necessary to get the call list.
19. Iceland	As a requesting State: The Ministry receives the MLA request either from the District Police Commissioners or from the Special Prosecutors Office. The Ministry guarantee that the request is sufficiently done and formally sends the request to the competent authority of the requested state.	As a *requested* State: All requests shall be sent to the Ministry of the Interior unless other arrangements are decided in an agreement with another state. The Ministry investigates the request and shall reject it if the legal conditions are not met or if it is clear that the request cannot be granted. If a request is not rejected the Ministry sends the case to the Director of Public Prosecutions for further treatment. The DPP orders the necessary investigation to be carried out, usually by the competent District Police Commissioner or the Special Prosecutors Office. When the investigation has been completed the DPP sends the evidence gathered to the Ministry, together with a report on it, and the Ministry forwards it to the competent authority in the requesting state.
20. Italy	As a *requesting* State: 1° Identification of information needed; 2° Submission of the request to the managing staff for approval; 3° Upon approval, sending of the request to the relevant contact point.	As a *requested* State: Absence of replies to mutual assistance requests in some cases. As a *requested* State: Late reception of requests, precluding authorities from preserving the data in time.

Country	Procedure for sending/receiving requests (Q 2.4)	Problems encountered (Q 2.5)
	As a *requested* State: The request is received, examined, evaluated and passed to the competent unit or division.	
21. Japan	As a *requesting* State: 1st situation: Request based on an MLA agreement Sending of the request to the foreign central authority by (a) the National Public Safety Commission (NPSC) for requests issued by a prefectural police, or (b) by the Ministry of Justice for requests issued by the office of the prosecutor; 2nd situation: Request not based on an MLA agreement Sending of the request to the foreign central authority by the Ministry of Foreign Affairs, upon request of the National Police Agency or the Ministry of Justice. As a *requested* State: 1st situation: Request based on an MLA agreement 1° Reception of the request by the Ministry of Justice; 2° Order by the MoJ to the competent authority (chief prosecutor; NPSC) to collect the evidence; 3° Sending of the collected evidence by the competent authority to the MoJ; 4° Forwarding of the evidence by the MoJ to the requesting State; 2nd situation: Request not based on an MLA agreement 1° Reception of the request by the Ministry of Foreign Affairs through diplomatic channels, which sends it to the MoJ; 2° Order by the MoJ to the competent authority (see above) to collect the evidence; 3° Sending of the collected evidence by the competent authority to the MoJ;	As a *requesting* State: Time required to receive the information requested. Example: Case involving illegal uploading of copyrighted work on foreign websites. Obtaining information (including upload log data) took 112 days, beyond the time limit set for the preservation of data by the ISP managing the IP addresses involved. It was thus not possible to track the subscriber information connected to these addresses. As a *requested* State: Lack of sufficient information provided in the request to justify the issuance of the court order necessary for search and seizure of data.

Country	Procedure for sending/receiving requests (Q 2.4)	Problems encountered (Q 2.5)
	4° Forwarding of the evidence to the Ministry of Foreign Affairs, which sends it to the diplomatic authority of the requesting State.	
22. Latvia	As a *requesting* State: 1° The person leading domestic proceedings transmits a written proposal (defining the form and content of request) to the competent authority to request a procedural action by the requested State; 2° Preparation of the request, containing documents required under domestic law (e.g. a court order, prosecutor accept) and respecting the applicable procedure; 3° If the request is considered justified, it is then translated and sent to the requested State. As a *requested* State: 1° Reception of the request for disclosure of stored data; 2° Decision of the competent authority on the admissibility of the procedural action needed; 3° Execution of the request in accordance with domestic law on criminal procedure (Nota: Material evidence needed, such as a media containing stored data, may be transmitted).	As a *requesting* State: Time needed to receive replies As a *requested* State: Problems are not identified
23. Lithuania	As a *requesting* State: 1° Preparation of the request by the national contact point; 2° (i) Sending of the request through the 24/7 network; (ii) preparation, in parallel, of the MLA request, which is then sent to the Prosecutor General's Office for follow-up. As a *requested* State: 1° Upon reception of a request for stored computer data, immediate application, by the national contact point, for the preservation of requested data by the ISP concerned;	As a *requesting* State: Lack of updated information on legislation; Formal requirements set by certain foreign States. As a *requested* State: No essential problems.

Country	Procedure for sending/receiving requests (Q 2.4)	Problems encountered (Q 2.5)
	2° Upon reception of the MLA request, all possible actions needed are performed.	
24. Moldova	(On the basis of international agreements or reciprocity) As a *requesting* State: (a) Transmission of the request, by the criminal prosecution body to the General Prosecutor, for submission for execution in the requested State; (b) Transmission of the request by the competent court to the Ministry of Justice, for submission for execution in the requested State. As a *requested* State: Upon reception of the request, forwarding of the request by (a) the General Prosecutor's Office to the criminal investigation body, or where appropriate (b) by the Ministry of Justice to the competent court; International agreements or reciprocal agreements may provide for specific procedures under the law of the requesting State, or the assistance of requesting authorities in the execution of the request; When the execution of the request is not possible, documents are returned to the requesting State, together with information justifying the refusal.	As a *requesting* State: Time issues (duration of the procedure; tight deadlines to handle evidence). Discrepancies between legal systems. As a *requested* State: Legal restrictions based on the protection of personal data; Time issues (duration of the procedure; tight deadlines to handle evidence). Discrepancies between legal systems. Need to improve the special techniques, institutional capacities of the personnel for cooperation and sharing of best practices and experiences in the field of cybercrime.
25. Montenegro	As a *requesting* State: (in the absence of international agreement) The authority seeking the data prepares a letter rogatory and transmits it to the Ministry of Justice; Upon completion of legal verifications, the Ministry of Justice sends the request to the requested State. As a *requested* State: Upon reception by the Ministry of Justice, transmission of the	As a *requesting* State: Lack of experience. As a *requested* State: Lack of experience.

Country	Procedure for sending/receiving requests (Q 2.4)	Problems encountered (Q 2.5)
	request to the competent judicial authority; The competent judicial authority executes the request and collect the data sought.	
26. Netherlands	As a *requesting* State: 1° Registration of the request, and sending to the national office for international legal assistance in criminal matters; 2° Formal sending of the request by the office, either (a) (EU countries) directly, or (b) (non-EU countries) via the central authority at the Ministry of Security and Justice. As a *requested* State: 1° Reception of the request through the 24/7 network, the Ministry of Security and Justice or the National Prosecutors' Office (NPO); 2° Examination of the request by the NPO, and decision with the high-tech crime team of the National Police, on who should execute the request: (a) regional units of the National Police, or (b) high-tech crime team; 3° Execution: (a) (regional units of the police) forwarding of the request to a local office for international assistance in criminal matters; (b) (high-tech crime team) forwarding of the request to the team, which registers it and names it; performance of a capacity check, and undertaking of actions needed to obtain applicable permissions from judicial authorities; sending of the results of the execution to the NPO. 4° Sending of results either directly to the requesting State, or via a judge.	As a *requesting* State: Time needed to translate requests. No knowledge of which authority is acting upon the request in the requested State. As a *requested* State: Extensive character of the request, creating high difficulties for its execution; Insufficient character of the research carried out (e.g. The requested State is not the relevant one for the data sought).
27. Norway	As a *requesting* State: 1° Identification of the State to whom the request should be addressed; 2° (a) (urgent cases) Direct sending of the request, with	As a *requesting* State: Time needed for processing requests (e.g. About one year to obtain content data in a specific murder case connected to organised crime); Discrepancies between legal systems;

Country	Procedure for sending/receiving requests (Q 2.4)	Problems encountered (Q 2.5)
	following sending of a formal request; (b) (common cases) Request by the prosecutor, to the domestic court, for a ruling stating that domestic legal requirements to access the data are met — to be sent together with the request. As a *requested* State: 1° Handling of the request by the prosecutor (typically at NCIS Norway/Kripos); 2° Identification of the target, clarification of the status of the person/company as a suspect or third party; 3° Issuance of a court order for the search or production of data (In urgent cases: Issuance of an order directly by the prosecutor, to be reviewed by the court later on). Certain types of data (e.g. customer information from an ISP) may be directly requested to the company; 4° Once the evidence is secured and/or analysed, the prosecutor and/or investigator often contact the requesting State to determine how the evidence should be transmitted; 5° If the Ministry of Justice received the initial request, the documents should be returned through the same channel.	Challenging identification of the target authority for the request (especially regarding web hosting services). As a *requested* State: Late reception of certain requests, especially regarding IP logs, deleted by ISPs after 21 days). Suggestion: Early contact by the requesting State to ensure that data be secured (via expedited preservation or parallel investigation).
28. Philippines	The procedure would depend on the particular Bilateral Agreement for mutual legal assistance on criminal matters between the Philippines and the particular country concerned.	As a requesting State: Complexity of the system As a requested State: Absence of a law.
29. Portugal	As a *requesting* State: 1° Transmission of the request to the Attorney General's Office (central authority for cooperation requests); 2° Sending of the request to the central authority of the requested State; 3° Reception of the reply by the channel of central authorities	As a *requesting* State: Lack of autonomy to request traffic data; Absence of the data sought in the requested State. As a *requested* State: Limited powers of the judicial police, which can only ask for the preservation of data.

Country	Procedure for sending/receiving requests (Q 2.4)	Problems encountered (Q 2.5)
	As a *requested* State: 1° Reception of the request by the Attorney General's Office; 2° Forwarding of the request to the Ministry of Justice for it to decide on its admissibility; 3° Sending of the request to the competent judicial authority, which executes the request – with the cooperation of the police if needed; 4° Following execution, forwarding of the reply by the judicial authority to the central authority, which sends it to the central authority of the requesting State. Nota: The Schengen Agreement allows for direct contact between judicial authorities, thus making the procedure shorter between its Parties.	
30. Romania	As a *requesting* State: 1° Preparation of the request by the Prosecutor carrying out criminal investigations and prosecution; 2° Submission of the request through the Office of International Legal Assistance (OILA) within the Directorate for Investigating Organized Crime and Terrorism (DIICOT) or within the General Prosecutor's Office, either (a) directly to the requested judicial authority (applicable in EU), or (b) to the central authority (e.g. Ministry of Justice). As a *requested* State: 1° Reception of the request through post, fax or email; 2° Registration of the request by the DIICOT or the General Prosecutor's Officer, and assignment to a prosecutor of the OILA; 3° Execution within the OILA, or sending for execution to the territorial offices and services of DIICOT or orther territorial prosecution office. For certain measures, the Prosecutor will have to ask for the approval of the competent judge (a specific	As a *requesting* State: Long time period required for the execution of requests (e.g. 3-6 months in certain States); Denial of requests on grounds of lack of seriousness/damage, or for budgetary reasons; In relation to interstate offences, requested judicial authorities should estimate the complexity of the investigation as a whole and not only in relation to the prejudice they suffered; Discrepancies between legal systems, especially regarding requirements for the interception and recording of communications, as well as for the house or computer search. As a *requested* State: Requests requiring data for which the time limit for data retention (six months) has expired.

Country	Procedure for sending/receiving requests (Q 2.4)	Problems encountered (Q 2.5)
	procedure applies to interception requests). In principle, the ISP or other data holder should provide the stored data within 48 hours. 4° Sending of the data obtained to the requesting authority.	
31. Serbia	As a *requesting* State: Request, by the prosecution, for the obtaining of data from the data holder (ISP or other legal person) with the assistance of the LEA. The foreign LEA contact point is immediately contacted. Where data cannot be obtained by these means, a formal rogatory letter is sent to foreign authorities. As a *requested* State: Upon reception of the request, initiation of the necessary measures; The prosecution executes the request through the LEA, ISP or other private entities; The obtained data is transmitted to the foreign judicial authority.	As a *requesting* State: Time issues (duration of the procedure; tight deadlines to handle evidence) Discrepancies between legal systems. As a *requested* State: Absence of the criminal offence in national law. Legal restrictions based on the protection of personal data. Time issues (duration of the procedure; tight deadlines to handle evidence). Discrepancies between legal systems.
32. Slovakia	As a requesting State: After the information from 24/7 contact point on preservation of data is provided, a prosecutor drafts a request for mutual legal assistance. A draft request is usually checked through by the Central Judicial Authority (General Prosecutor´s Office). Official translation is made by a competent translator. Finally a request is sent by channels and means available (based on the conditions of applicable treaty). As a requested State: Once a request is received, it is sent to the prosecution service (General Prosecutor´s Office, lower prosecution office). The content of a request (as well as the competence of a requested authority to issue such request) is examined by the prosecutor,	As a requesting State: First of all, it is important to receive information on the preservation of data as soon as possible with relevant references to the case in the requested state. As a requested State: It is important that the MLA request comes with a sufficient description of the offence, names of persons involved, places and dates of the offence, the damage caused, links to Slovakia, the letter should be properly signed and stamped, if available. For some actions, judicial orders are necessary and dual criminality requirements must be met. Therefore the proper information on the case is very important to satisfy domestic requirements.

Country	Procedure for sending/receiving requests (Q 2.4)	Problems encountered (Q 2.5)
	who decides on further steps (he or she has to provide for official translation, if a request is not delivered in Slovak, he or she may request additional information, authorize police to take some action, to make a motion to the court, where necessary).	
33. Slovenia	As a *requesting* State: 1° Transmission of the request by the competent police unit to the International Police Cooperation Sector (IPCS); 2° Translation of the request, which is then sent to the requested State. As a *requested* State: 1° Reception of the request by the IPCS, which translates it into Slovenian; 2° Assignment of the request to the competent police unit; 3° Implementation of preservation measures, if requested and possible; 4° Obtaining of the data with an official police letter or a court order, and sending to the requesting State.	As a *requesting* State: Time needed before a reply is send by the requested State; Absence of reply by the requesting State. As a *requested* State: In some instances, reluctance of judicial authorities to apply the provisions of the Cybercrime Convention, who favour MLA requests.
34. Spain	As a *requesting* State: 1° Transmission of the request to the Ministry of Justice; 2° Following legal verifications, (a) (where standards are not met) the request is sent back to the requesting authority, which should complete it; (b)(where standards are met) the request is forwarded to the central authority of the requested State. As a *requested* State: 1° Reception of the request by the Ministry of Justice; 2° Following legal verifications by the MoJ, transmission of the request for its execution to the competent judicial authority.	As a *requesting* State: Difficulty to provide the great amount of information required by the requested State, especially since most requests are sent at an early stage; As a *requested* State: No specific problems.
35. Switzerland	As a *requesting* State: 1° Summary examination (translation, etc.);	As a *requesting* State: Absence of confirmation of reception of the request;

Country	Procedure for sending/receiving requests (Q 2.4)	Problems encountered (Q 2.5)
	2° Request of measures (only measures that domestic authorities could grant themselves). As a *requested* State: 1° Summary examination (translation, requesting authority); 2° Appointment of the competent LEA (federal or cantonal prosecutor); 3° Issuance of the initial decree (conditions: respect of double criminality principle, proportionality and approval of the court where necessary); 4° Obtaining of the data; 5° Issuance of the final decree; 6° Ev. legal remedies.	Diverging criteria set to qualify a request as "urgent". As a *requested* State: Insufficient presentation of the facts (modus operandi); The request regards data stored for more than six months (i.e. beyond the time set during which ISPs are required to stored data).
36. "The former Yugoslav Republic of Macedonia"	As a *requesting* State: The request of the competent court is transmitted via diplomatic channels (Ministry to the foreign authorities) As a *requested* State: The request of the foreign authorities is delivered by the Ministry of Foreign Affairs to the Ministry of Justice; The MoJ transmits it to the competent court for its execution; In case of emergency, the Ministry of Interior may handle directly requests (condition: reciprocity).	As a *requesting* State: N/a. As a *requested* State: N/a.
37. Turkey	As a *requesting* State: Preparation of the request by the prosecutor, who transmits it to the central authority; Upon completion of legal verifications, the request is sent to the foreign authority. As a *requested* State:	As a *requesting* State: Time issues (duration of the procedure; tight deadlines to handle evidence) Discrepancies between legal systems. Difficulty of cooperation with certain ISPs. Problems regarding the functioning of contact point cooperation. Lack of satisfactory translation.

Country	Procedure for sending/receiving requests (Q 2.4)	Problems encountered (Q 2.5)
	The central authority (General Directorate of International Law and Foreign Relations) receives the request; It transmits the request to the competent authority; The local prosecutor executes the request, by directly issuing an order to the ISP (subscriber data), or via a court order (traffic and content data) issued by a judge. Once the data is obtained from the ISP, the data is sent to the central authority, which transmits it to the requesting State.	As a *requested* State: N/a.
38. Ukraine	(MoI) As a *requesting* State: 1° Approval of the prosecutor; 2° Sending of the request by a competent authority (judge, prosecutor or investigator) to the competent (central) authority on mutual assistance; 3° Following legal verifications, sending of the request within 10 days by the competent (central) authority to the competent authority of the requested State, either directly or through diplomatic channels; 4° Upon denial of the request, return of all documents within 10 days, and details explaining the denial. As a *requested* State (procedure for temporary access): 1° Upon reception of a request, issuance of an order by the investigative judge, upon approval by the prosecutor; 2° Execution of the order and obtaining of the requested data from the relevant legal/natural person holding it. (Sec Serv) As a *requesting* State: 1° Sending of the request to the General Prosecutor's Office (GPO); 2° Verification of its compliance with domestic and international	(MoI) As a *requesting* State: Short terms to carry out the request (one month, with possibility of authorised continuation). As a *requested* State: No problems. (Sec Serv) As a *requesting* State: Classified character of the results of investigations undertaken by accessing to a computer system without its owner's approval ('undercover investigation action'), which transfer to a foreign State entails a complex procedure; Short term (1 month) As a *requested* State: Discrepancies between legislations.

Country	Procedure for sending/receiving requests (Q 2.4)	Problems encountered (Q 2.5)
	legal requirements by the GPO; 3° Sending of the request (within ten days) by the GPO to the requested State, via diplomatic or other channels. As a *requested* State: 1° Upon reception of the request, examination of legal requirements by the GPO, and identification of the competent LEA for the execution; 2° Measures are taken by the competent LEA during one month (or longer if necessary) to execute the request, and the materials forwarded to the GPO; 3° Sending of the reply (materials obtained or reasons for failure to execute) by the GPO to the requesting State.	
39. United Kingdom	As a *requesting* State: Dependent on the requirements of the requested State. The necessary character and proportionality of the request is assessed by domestic authorities. As a *requested* State: [Problem: Reference to a "link below" [to be clarified]]	As a *requesting* State: [Lack of information on] whether the data has been retained and is available. Time taken to obtain the data. As a *requested* State: Issues of terminology; discrepancies in the legal language used.
40. United States of America	As a *requesting* State: 1° Submission, by the investigation or prosecuting authority seeking the data, of a draft request to the Office of International Affairs (OIA); 2° Review and editing of the request by the OIA; 3° Following legal verifications, the OIA approves the request, signs it and transmits it directly to the central authority of the requested State. As a *requested* State: 1° Review of the request by the OIA, determining whether the data is preserved and the legal and factual basis sufficient to	As a *requesting* State: Delays in the execution of the request; Inadequacy of law of the requested State; Lack of knowledge/training of the requested State's central authority on high-tech issues; Lack of staff in the requested State; Lack of awareness of the increasing importance of electronic evidence, and of a proper reaction to this evolution. As a *requested* State: Delays of the requesting State in sending the request (when preservation has not been sought, the data is likely to have been destroyed at the time of

Country	Procedure for sending/receiving requests (Q 2.4)	Problems encountered (Q 2.5)
	obtain the data; (Additional steps: Preservation of data if it has not been done already; if the legal and factual basis is not sufficient, discussion and request for further information.) 2° Transmission of the request to the competent federal prosecutor's office to obtain a court order; 3° Issuance of the court order and production of the data; 4° Review of the responsiveness of the data and forwarding to the requesting State through MLA channels.	reception of the request); Lack of knowledge of domestic requirements for obtaining evidence; Failure to meet domestic requirements; Slowness of the domestic authorities in executing the requests (overburden).

4 Assessment of channels and means of cooperation

4.1 Authorities, channels and means of cooperation

Chapter III of the Budapest Convention does not supersede other bi- or multi-lateral agreements or arrangements for international cooperation that a Party has entered into, but encourages the use of such agreements and arrangements for cooperation on cybercrime and electronic evidence:

> Article 23 – General principles relating to international co-operation
>
> The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Parties shall, therefore, make use of such agreements and arrangements for mutual assistance requests regarding stored computer data:

> Article 31 – Mutual assistance regarding accessing of stored computer data
>
> 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.

Most States thus allow for different authorities depending on the agreement used in a specific case. For example, 36 Parties to the Budapest Convention are Parties to the European Convention on Cooperation in Criminal Matters (ETS 30)[18], and 28 are Parties to the 2nd Additional to this treaty (ETS 182).[19] This Protocol, among other things, allows for direct cooperation between judicial authorities:

> ETS 182: Article 4 – Channels of communication
>
> Article 15 of the Convention shall be replaced by the following provisions:
> "1 Requests for mutual assistance, as well as spontaneous information, shall be addressed in writing by the Ministry of Justice of the requesting Party to the Ministry of Justice of the requested Party and shall be returned through the same channels. However, they may be forwarded directly by the judicial authorities of the requesting Party to the judicial authorities of the requested Party and returned through the same channels.

---

[18] http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=030&CM=8&DF=&CL=ENG
Parties to ETS 30 also include Chile and Israel which have been invited to accede to the Budapest Convention. Furthermore, Korea is a Party and Brazil and South Africa have been invited to accede.

[19] http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=182&CM=8&DF=&CL=ENG
Parties to ETS 182 also include Chile and Israel which have been invited to accede to the Budapest Convention.

Under Article 6 ETS 182, Parties shall declare which authorities they deem judicial authorities. Many Parties have defined a range of judicial authorities, including ministries of justice, prosecution services and courts, but often also investigative authorities.[20]

In the absence of such agreements and arrangements, Parties to the Budapest Convention shall apply the procedures foreseen in Article 27.[21] For the purposes of Article 27, Parties shall also designate central authorities for sending and receiving requests for mutual assistance.

Replies to the questionnaire indicate that some States allow for multiple channels while others follow a more limited approach:

- Diplomatic channels: Australia, Philippines, Ukraine.
- Ministry of Justice: Albania, Turkey.
- Office of Prosecutor General: Armenia, Dominican Republic.
- Multiple channels: Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Finland, Georgia, Latvia, Lithuania, Romania, Switzerland, "The former Yugoslav Republic of Macedonia".

Article 25.3 allows for expedited means of communication in urgent circumstances:

> Article 25 – General principles relating to mutual assistance
>
> 3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

Replies to the questionnaire suggest that the use of email or fax is not limited to urgent cases but is accepted in all circumstances by most Parties. Some require that formal written documentation is submitted in addition.

Preliminary conclusions:

- Channels and authorities for Article 31-type requests should be used in a flexible and pragmatic manner. Parties should clarify in broad terms which channels and authorities are accepted for such requests.
- Direct contacts should be favoured.

---

[20] http://conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?NT=182&CM=8&DF=03/11/2013&CL=ENG&VL=1

[21] Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

- An online platform listing central and judicial authorities and requirements would be useful.

- Central authorities and 24/7 points of contact should provide guidance with respect to the relevant authorities in a Party that could be contacted directly.

4.2 Urgent requests/expedited responses

Article 31 foresees expedited responses to requests for mutual assistance:

> Article 31 – Mutual assistance regarding accessing of stored computer data
>
> 3 The request shall be responded to on an expedited basis where:
> a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or
> b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

Parties apply different criteria to consider a request as "urgent". A request is considered urgent if it relates to:

- imminent danger for life and health, substantial material damage, imminent attack on critical infrastructure or similar: Albania, Belgium, Bosnia and Herzegovina, Estonia, Finland, Germany, Netherlands, Norway, Serbia, Slovenia, Spain, Turkey, UK, USA;

- risk of loss or modification of data: Austria, Bosnia and Herzegovina, Cyprus, France, Germany, Latvia, Moldova, Norway, Romania, Slovakia, Spain, Switzerland, Turkey, Ukraine, USA;

- any request regarding a cybercrime offence: Croatia;

- other considerations (e.g. pressing timeframe, nature of the offence, ongoing custody, prevention of a specific crime): Australia, Costa Rica, Georgia, France, Italy, Moldova, Portugal, Romania, Finland and USA.

A number of Parties indicate that they would evaluate the urgency of requests case by case (Estonia, Georgia, Lithuania).

For urgent requests, many Parties foresee specific mechanisms, procedures or channels. For example:

- Use of 24/7 point of contact, liaison officers, judicial networks (including EUROJUST and European Judicial Network), channels for police cooperation (including also INTERPOL) and similar: Albania, Australia, Austria, Belgium, Bosnia and Herzegovina, Bulgaria, Cyprus, Dominican Republic, Estonia, Finland, France, Latvia, Lithuania, Netherlands, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Turkey, USA.

- Direct communication by phone, email or fax, including advance contact of foreign authorities to alert them of impending request: Albania, Australia, Costa Rica, Georgia, Germany, Romania, Serbia, Spain, Switzerland.

- Direct contact to foreign judicial authorities: Austria, Belgium, Slovakia.

- Giving priority to requests marked "urgent": Albania, Hungary, Romania, and Spain.

- Other arrangements: in Norway, as a requested State, a prosecutor may issue a search or production order without court approval if the request substantiates the urgency.

4.3 Role of 24/7 point of contact

Under Article 35, Parties shall establish 24/7 points of contact "in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence."

Article 35 does not specifically stipulate a role of 24/7 contact points for mutual assistance requests pertaining to Article 31, but also does not exclude such a role. Article 35.2.b states:

> 2.b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

Question 3.2.1 therefore inquired about the competence of 24/7 contact points regarding mutual assistance requests and question 3.2.2 about the coordination of contact points with competent authorities for mutual assistance to expedite the execution of requests in line with Article 35.2.b.

The contact points of approximately half of the States that replied have the competence to send or receive requests for mutual assistance. Some of these may serve as channels for transmission only (such as Bosnia and Herzegovina, Estonia, Hungary, and Netherlands).

Others can also issue rogatory letters or execute (or supervise or participate in the execution of) requests for mutual assistance (Costa Rica, Cyprus, Finland, Georgia, Lithuania, Norway, Romania, Serbia, "The former Yugoslav Republic of Macedonia", United Kingdom).

Direct communication and regular liaison between 24/7 contact points and authorities responsible for executing MLA requests have been reported by Albania, Armenia, Australia, Austria, Bulgaria, Estonia, Japan, Netherlands, Romania, Slovakia.

In a number of States, however, there seems to be the risk of disconnect between contact points and MLA authorities. For example, contact points are not informed as to whether preservation requests are followed up to by MLA requests; or practical arrangements have not yet been established regarding the expedited coordination between contact points and MLA authorities.

Preliminary conclusion:

- 24/7 points of contact – unless they have themselves the authority to send, receive or execute Article 31-type MLA requests – should have the capability to facilitate swift execution of MLA requests.

State	Competence for sending/receiving requests
1. Albania	YES
2. Armenia	NO
3. Australia	NO
4. Austria	NO
5. Azerbaijan	YES
6. Belgium	NO
7. Bosnia and Herzegovina	YES (transmission through INTERPOL channels; use of Eurojust)
8. Bulgaria	NO
9. Costa Rica	YES
10. Croatia	NO
11. Cyprus	YES
12. Denmark	
13. Dominican Republic	
14. Estonia	YES (transmission only)
15. Finland	YES (in matters falling in its competence)
16. France	NO
17. Georgia	YES
18. Germany	NO
19. Hungary	YES (transmission only)
20. Iceland	
21. Italy	
22. Japan	NO
23. Latvia	NO
24. Lithuania	YES
25. Malta	
26. Moldova	NO
27. Montenegro	YES [to be confirmed]
28. Netherlands	YES (transmission only)
29. Norway	YES
30. Philippines	YES (transmission only)
31. Portugal	NO
32. Romania	YES
33. Serbia	YES
34. Slovakia	NO (but facilitate transmission)
35. Slovenia	serve as a channel for transmission
36. Spain	[to be clarified]
37. Switzerland	
38. "The former Yugoslav Republic of Macedonia"	YES
39. Turkey	NO
40. Ukraine	NO
41. United Kingdom	YES
42. United States of America	NO (but facilitate transmission)

4.4 Direct contact to obtain data from physical or legal persons in foreign jurisdictions

With respect to the possibility to contact holders of data (physical or legal persons such as Internet service providers) in foreign jurisdictions directly to obtain stored data, a few States consider this not allowed under their domestic law, while in most others this is not regulated or is allowed.

In practice, the prosecution or police services of many States contact foreign service providers directly.[22] Where these have a legal representation in the territory of the requesting authority, requests may take the form of a domestic production order even if the data is physically stored abroad. In some instances, law enforcement authorities have agreements with foreign service providers.

Foreign service providers may respond positively to a request under certain conditions. For example:

- Disclosure of data must be allowed under the domestic law of the service provider (US providers are allowed to disclose traffic or subscriber data but not content data) as otherwise administrative or criminal sanctions may apply.
- The request must be lawful (e.g. production order).
- However, increasingly, providers may require that the request relate to the jurisdiction of the requesting authority (for example, relate to persons or IP addresses in the territory of the requesting authority).

Moreover, some providers have established specific procedures to respond to emergency requests (such as threats to life and limb).

Replies suggest that often information thus obtained cannot be used as evidence in court proceedings and would need to be formalised through a subsequent mutual assistance request.

[22] Transparency reports by companies such as Facebook, Google, Microsoft or Yahoo show that at least half of the Parties to the Budapest Convention submit requests. In almost all cases these are regarding subscriber or traffic data.
https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/
https://www.google.com/transparencyreport/?hl=en-US
http://l.yimg.com/pj/info/tr/Yahoo_Transparency_Report-Jan-June-2013-1.3.pdf
https://www.facebook.com/about/government_requests

4.5 Coordination in complex international cases

With regard to mechanisms to coordinate complex international cases, States refer to:

- use of EUROPOL, EUROJUST or INTERPOL;
- the setting of joint investigation teams (sometimes this is subject to agreements in force);
- use of law enforcement liaison officers or networks.

Preliminary conclusion:

- It may be worth considering to include a provision on joint investigation teams into a Protocol to the Budapest Convention similar to Article 20 of ETS 182[23]

[23] http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=182&CM=8&DF=&CL=ENG

4.6 Tables on questions 3.1 – 3.4

4.6.1 Authorities (Question 3.1.1)

Country	MLA authority in the absence of other treaties (article 27)	Authority for extradition and provisional arrests in the absence of other treaties (article 24)	24/7 point of contact (article 35)
1. Albania	Ministry of Justice, Bulevardi Zog. I., Tirana	Ministry of Justice, Bulevardi Zog. I., Tirana National Central Office of Interpol, Bulevardi Deshmoret e Kombit, Tirana	Sector against Computer Crime, Ministry of Interior Tirana, Albania
2. Armenia	Main Department on Combat Against Organized Crime of the Police of the Republic of Armenia	Main Department on Combat Against Organized Crime of the Police of the Republic of Armenia	Division on High-tech Crime, Main Department on Combat Against Organized Crime of the Police of the Republic of Armenia
3. Australia	International Crime Cooperation Central Authority Attorney-General's Department 3-5 National Circuit Barton ACT 2600 Australia	International Crime Cooperation Central Authority Attorney-General's Department 3-5 National Circuit Barton ACT 2600 Australia	AOCC Watchfloor Operations Australian Federal police GPO Box 401 Canberra ACT 2601 Australia
4. Austria	*Bundesministerium für Justiz* (Federal Ministry of Justice) Abt. IV 4 *Internationale Strafsachen* (International Criminal Matters) 1070 Wien, Museumstrasse 7 Tel.: +43 1 52 1 52-0 E-Mail: team.s@bmj.gv.at	*Bundesministerium für Justiz* (Federal Ministry of Justice) Abt. IV 4 *Internationale Strafsachen* (International Criminal Matters) 1070 Wien, Museumstrasse 7 Tel.: +43 1 52 1 52-0 E-Mail: team.s@bmj.gv.at z	*Bundesministerium für Inneres* (Federal Ministry of the Interior) *Bundeskriminalamt* (Federal Criminal Police Office) Büro 5.2 Cyber-Crime-Competence-Center Josef Holaubek Platz 1 1090 Wien
5. Azerbaijan	Ministry of National Security Address: 2, Parliament Avenue, Baky, AZ 1006, Republic of Azerbaijan; e-mail:	Ministry of Justice Address: 1, Inshaatchilar Avenue, Baky, AZ 1073, Republic of Azerbaijan; e-mail:	Department of Combating Crimes in Communications and IT Sphere, Ministry of National Security

Country	MLA authority in the absence of other treaties (article 27)	Authority for extradition and provisional arrests in the absence of other treaties (article 24)	24/7 point of contact (article 35)
	secretoffice@mns.gov.az	contact@justice.gov.az	
6. Belgium	Service Public Fédéral Justice Service de la coopération internationale pénale Boulevard de Waterloo 115 1000 Bruxelles Fax : +32(0)2/210.57.98	Service Public Fédéral Justice Service de la coopération internationale pénale Boulevard de Waterloo 115 1000 Bruxelles Fax : +32(0)2/210.57.98	Federal Computer Crime Unit
7. Bosnia and Herzegovina	Ministry of Justice of Bosnia and Herzegovina	Ministry of Justice of Bosnia and Herzegovina	Directorate for Coordination of Police Bodies of Bosnia and Herzegovina (International Police Cooperation Sector - Interpol)
8. Bulgaria	Ministry of Justice (trial stage), Supreme Cassation Prosecutor's Office (pre-trial stage)	Ministry of Justice (extradition), Supreme Cassation Prosecutor's Office (provisional arrests)	National Service for Combating Organized Crime under the Ministry of Interior
9. Costa Rica			
10. Croatia	Ministry of Justice of the Republic of Croatia Vukovarska Street 49 10 000 Zagreb	Ministry of Justice of the Republic of Croatia Vukovarska Street 49 10 000 Zagreb	Ministry of Interior, Police - Directorate for crime police, Ilica 335, 10 000 Zagreb
11. Cyprus	Ministry of Justice and Public Order Athalassas Av. 125 1461 NICOSIA	Ministry of Justice and Public Order Athalassas Av. 125 1461 NICOSIA	Office for Combating Cybercrime and Forensic Laboratory, Cyprus Police Headquarters Ministry of Justice and Public Order Athalassas Av. 125 1461 NICOSIA
12. Denmark	Ministry of Justice, Slotsholmsgade 10, DK-1216 Copenhagen K, Denmark	Ministry of Justice, Slotsholmsgade 10, DK-1216 Copenhagen K, Denmark	Danish National Police, Police Department, Polititorvet 14, DK-1780 Copenhagen V, Denmark
13. Dominican	Procuradoria General de la Republica	Procuradoria General de la Republica	High Tech Crimes Investigation Department (DICAT), National Police, Santo Domingo,

Country	MLA authority in the absence of other treaties (article 27)	Authority for extradition and provisional arrests in the absence of other treaties (article 24)	24/7 point of contact (article 35)
Republic	and High Tech Crimes Investigation Department (DICAT), National Police	and High Tech Crimes Investigation Department (DICAT), National Police	Dominican Republic
14. Estonia	Ministry of Justice	Ministry of Justice	Bureau of Criminal Intelligence, Criminal Police Department
15. Finland	Ministry of Justice, Eteläesplanadi 10, FIN-00130 Helsinki	For requests for extradition, the Ministry of Justice, Eteläesplanadi 10, FIN-00130 Helsinki For requests for provisional arrest, the National Bureau of Investigation, Jokiniemenkuja 4, FIN-01370 Vantaa	National Bureau of Investigation, International Affairs / Communications Centre
16. France	From French judicial authorities directed to foreign judicial authorities transmitted through the Ministry of Justice (*Ministère de la Justice, 13, Place Vendôme, 75042 Paris Cedex 01*) From foreign judicial authorities directed to French judicial authorities are transmitted through diplomatic channels (*Ministère des Affaires étrangères, 37, Quai d'Orsay, 75700 Paris 07 SP*)	Ministry for Foreign Affairs for extradition (*Ministère des Affaires étrangères, 37, Quai d'Orsay, 75700 Paris 07 SP*); The territorially competent State Prosecutor for requests for provisional arrest	Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication" (11, Rue des Saussaies, 75800 Paris)
17. Georgia	Ministry of Justice of Georgia 24a Gorgasali str. Tbilisi 0114 - Georgia	Ministry of Justice of Georgia 24a Gorgasali str. Tbilisi 0114 - Georgia	Cybercrime Unit Ministry of Internal Affairs of Georgia Criminal Police Department 10 G. Gulua str. Tbilisi 0114 - Georgia
18. Germany	Ministry of Foreign Affairs Address: Auswärtiges Amt, Werderscher Markt 1, 10117 Berlin	Ministry of Foreign Affairs Address: Auswärtiges Amt, Werderscher Markt 1, 10117 Berlin	National High Tech Crime Unit at the Federal Criminal Police Office 65193 Wiesbaden
19. Hungary	Before starting the criminal procedure: International Law Enforcement Cooperation Centre Budapest, Teve u. 4-6 1139 - Hungary	Ministry of Justice for extradition or provisional arrest. The National Central Bureau of Interpol for provisional arrest.	International Law Enforcement Cooperation Centre, Police

Country	MLA authority in the absence of other treaties (article 27)	Authority for extradition and provisional arrests in the absence of other treaties (article 24)	24/7 point of contact (article 35)
	After starting the criminal procedure: the General Prosecutor's Office of the Republic of Hungary Budapest, Markó u. 4-6 1055 - Hungary		Alternative: High Tech Crime Unit, National Bureau of Investigations
20. Iceland	Ministry of the Interior Sölvhólsgötu 7 IS-150 Reykjavík Iceland Tel.: +354 545-9000 Fax: +354 552-7340 Email: postur@irr.is	Ministry of the Interior Sölvhólsgötu 7 IS-150 Reykjavík Iceland Tel.: +354 545-9000 Fax: +354 552-7340 Email: postur@irr.is	National Commissioner of the Icelandic Police (Ríkislögreglustjórinn), Skúlagata 21, 101 Reykjavík, Iceland
21. Italy	Ministry of Justice Department for Affairs of Justice Directorate General of Criminal Justice Office II (International Judicial Cooperation) Viale Arenula 70 I - 00186 ROMA	Ministry of Justice Department for Affairs of Justice Directorate General of Criminal Justice Office II (International Judicial Cooperation) Viale Arenula 70 I - 00186 ROMA	Servizio Polizia Postale e delle Comunicazioni Ministry of the Interior Alternative: Office of District Attorney of Rome –Cybercrime Section
22. Japan	The Minister of Justice or the person designated by the Minister (Director of International Affairs Division) and The National Public Safety Commission or the person designated by the Commission (Director of International Investigative Operations Division) Organized Crime Department National Police Agency 2-1-2, Kasumigaseki Chiyoda-ku Tokyo 100-8974	The Minister for Foreign Affairs 2-2-1, Kasumigaseki Chiyoda-ku Tokyo 100-8919	International Investigative Operations Division Organized Crime Department National Police Agency 2-1-2, Kasumigaseki Chiyoda-ku Tokyo 100-8974

Country	MLA authority in the absence of other treaties (article 27)	Authority for extradition and provisional arrests in the absence of other treaties (article 24)	24/7 point of contact (article 35)
23. Latvia	Ministry of Justice Brivibas Blvd. 36, Riga LV-1536, Latvia	Prosecutor General Office Kalpaka Blvd. 6, Riga LV-1801, Latvia	International Cooperation Department of Central Criminal Police Department of State Police Ciekurkalna 1.linija 1, k-4, Riga LV-1026, Latvia
24. Lithuania	Ministry of Justice and the General Prosecutor's Office of the Republic of Lithuania	Ministry of Justice and the General Prosecutor's Office of the Republic of Lithuania	Police Department under the Ministry of the Interior of the Republic of Lithuania
25. Malta	The Office of the Attorney General The Palace Valletta Malta Email: ag.mla@gov.mt	The Ministry for Justice Office of the Prime Minister Auberge de Castille Valletta VLT 2000 Malta	Cybercrime Unit Malta Police Police General Headquarters Floriana Malta
26. Moldova	Office of the Prosecutor General in the phase of penal prosecution: 26, Banulescu - Bodoni str., MD-2012 Chisinau, Republic of Moldova. Ministry of Justice in the judiciary phase or the execution of punishment: 82, 31 August 1989 str., MD-2012 Chisinau, Republic of Moldova.	Office of the Prosecutor General in the phase of penal prosecution: 26, Banulescu - Bodoni str., MD-2012 Chisinau, Republic of Moldova. Ministry of Justice in the judiciary phase or the execution of punishment: 82, 31 August 1989 str., MD-2012 Chisinau, Republic of Moldova.	Department of Information Technology and Investigation Cyber Crime General Prosecutor Office: 26, Banulescu - Bodoni str., MD-2012 Chisinau, Republic of Moldova. Direction of Prevention and Combating of Cybernetic, Information and Transnational Offences of the Ministry of Internal Affairs: 14, Bucuriei str., MD-2004 Chisinau, Republic of Moldova.
27. Montenegro	Ministry of Justice of Montenegro, address: Vuka Karadžica 3, 81 000 Podgorica	Ministry of Justice of Montenegro, address: Vuka Karadžica 3, 81 000 Podgorica For provisional arrest in the absence of an agreement: NCB Interpol in Podgorica, address: Bulevar Svetog Petra Cetinjskog 22, 81 000	Inspector for fighting cybercrime Police Directorate of Montenegro
28. Netherlands	*Landelijk Parket van het openbaar ministerie* (National office of the public prosecution service)	The Ministry of Security and Justice Office of International Legal Assistance in Criminal Matters	*Landelijk Parket van het openbaar ministerie* (National office of the public prosecution

Country	MLA authority in the absence of other treaties (article 27)	Authority for extradition and provisional arrests in the absence of other treaties (article 24)	24/7 point of contact (article 35)
	Postbus 395 3000 AJ ROTTERDAM	PO BOX 20301 2500 EH THE HAGUE	service) Postbus 395 3000 AJ ROTTERDAM
29. Norway	The National Criminal Investigation Service (KRIPOS)	Royal Ministry of Justice and the Police, P.O. Box 8005, N-0030 OSLO	High Tech Crime Division National Criminal Investigation Service (KRIPOS)
30. Philippines	Department of Justice		Department of Justice – Office of Cybercrime
31. Portugal	*Procuradoria-Geral da República* (Rua da Escola Politécnica, 140 – 1269-269 Lisboa, Portugal	*Procuradoria-Geral da República* (Rua da Escola Politécnica, 140 – 1269-269 Lisboa, Portugal)	Judiciary Police (*Polícia Judiciária*) Rua Gomes Freire, 174 1169-007 Lisboa Portugal
32. Romania	The Prosecutor's Office to the High Court of Cassation and Justice for pre-trial investigations (address: Blvd. Libertatii nr. 12-14, sector 5, Bucuresti) The Ministry of Justice for the requests during the trial or execution of punishment Ministry of Justice, Directorate International Law and Judicial Cooperation, Service for International Judicial Cooperation in Criminal Matters, Apolodor Street No. 17, Sector 5, 050741	Ministry of Justice (address: Str. Apollodor nr. 17, sector 5, Bucuresti) Extradition itself is granted by Courts.	Service of Combating Cybercrime within the Directorate for investigation of Organized Crime and Terrorism Offences/ Prosecutor's Office attached to the High Court of Cassation and Justice (address: Blvd. Libertatii nr. 12-14, sector 5, Bucuresti).
33. Serbia	District Attorney for High-Tech Crime of the Republic of Serbia Savska 17A 11000 Beograd Ministry of Interior of the Republic of Serbia Directorate of Crime Police	District Attorney for High-Tech Crime of the Republic of Serbia Savska 17A 11000 Beograd Ministry of Interior of the Republic of Serbia Directorate of Crime Police	District Attorney for High-Tech Crime of the Republic of Serbia Savska 17A 11000 Beograd Ministry of Interior of the Republic of Serbia Directorate of Crime Police Department for the fight against organized

Country	MLA authority in the absence of other treaties (article 27)	Authority for extradition and provisional arrests in the absence of other treaties (article 24)	24/7 point of contact (article 35)
	Department for the fight against organized crime Bulevar Mihajla Pupina 2 11070 Novi Beograd	Department for the fight against organized crime Bulevar Mihajla Pupina 2 11070 Novi Beograd	crime Bulevar Mihajla Pupina 2 11070 Novi Beograd
34. Slovakia	Ministry of Justice of the Slovak Republic (Zupné námestie 13, 81311 Bratislava) and the General Prosecutor's Office (Stúrova 2, 81285 Bratislava)	Ministry of Justice of the Slovak Republic (Zupné námestie 13, 81311 Bratislava) for extradition Competent prosecutor of the Regional Prosecutor's Office and the Ministry of Justice for receiving requests for provisional arrests Ministry of Justice of the Slovak Republic and the court competent for issuing an international arrest warrant	National Central Bureau Interpol Vajnorská 25812 72 BratislavaSlovakia
35. Slovenia	Ministry of Justice Zupanciceva 3 SI - 1000 Ljubljana	Ministry of Foreign Affairs for extradition: Presernova 25 SI - 1000 Ljubljana Ministry of the Interior, Criminal Investigation Police Directorate, International Police Cooperation Section for requests for provisional arrests: Ministry of the Interior Criminal Investigation Police Directorate International Police Cooperation Section	Ministry of the Interior Criminal Investigation Police Directorate International Police Cooperation Section Alternative: Cyber Investigation Unit, Criminal Police Directorate
36. Spain	Sub-Directorate General for International Legal Cooperation of the Ministry of Justice San Bernardo 62, 28071, Madrid	Sub-Directorate General for International Legal Cooperation of the Ministry of Justice San Bernardo 62, 28071, Madrid	High Technological Investigation Unit of the National Police Comisaria General de Policia Judicial, Brigada de Investigación Tecnológica (CGPJ), C/ Julián González Segador s/n 28071 Madrid

Country	MLA authority in the absence of other treaties (article 27)	Authority for extradition and provisional arrests in the absence of other treaties (article 24)	24/7 point of contact (article 35)
37. Switzerland	Federal Office of Justice, the Federal Department of Justice and Police, 3003 Berne	Federal Office of Justice, the Federal Department of Justice and Police, 3003 Berne	Operations Centre FEDPOL Federal Office of Justice
38. "The former Yugoslav Republic of Macedonia"	Ministry of Justice	Ministry of Justice	Basic Public Prosecutor‘s Office Skopje Alternative: Cybercrime Unit, Ministry of Interior
39. Turkey			
40. Ukraine	Ministry of Justice of Ukraine (concerning courts' commission) and the General Prosecutor's Office of Ukraine (concerning commissions of bodies of prejudicial inquiry)	Ministry of Justice of Ukraine (concerning court's inquiries) and the General Prosecutor's Office of Ukraine (concerning inquiries of bodies of prejudicial inquiry)	Division for Combating Cybercrime, Ministry of Internal Affairs
41. United Kingdom	For matters related to England, Wales, and Northern Ireland: UK Central Authority Home Office, 5th Floor Peel building 2 Marsham Street London, SW1P 4DF For matters related to Scotland: International Co-operation Unit Argyle House C Floor 3 Lady Lawson Street Edinburgh, EH3 9DR For matters related to indirect taxation: Law Enforcement & International Advisory Division HM Revenue and Customs – Solicitor’s	Home Office Judicial Co-operation Unit 5th Floor, Fry building 2 Marsham Street London SW1P 4DF Scottish Government (when the person is believed to be in Scotland) Criminal Procedure Division St. Andrew’s House Regent Road Edinburgh EH1 3DG	Cyber Duty Officer SOCA Cyber

Country	MLA authority in the absence of other treaties (article 27)	Authority for extradition and provisional arrests in the absence of other treaties (article 24)	24/7 point of contact (article 35)
	Office, Room 2/74 100 Parliament Street London, SW1A 2BQ		
42. USA	Office of International Affairs, United States Department of Justice, Criminal Division, Washington, D.C., 20530		Computer Crime and Intellectual Property Section (CCIPS) U.S. Department of Justice, Washington, DC

4.6.2 Channels and means of cooperation (Question 3.1)

3.1.2 Which channels, procedures and means (fax, email or other) of cooperation do you normally use to request stored computer data by mutual assistance in another State? 3.1.3 What are criteria to consider a request "urgent"? 3.1.4 As a requesting State: Do you use different mechanisms, procedures or channels if you consider your request for data "urgent"? 3.1.5 As a requested State: Do you use different mechanisms, procedures or channels to execute a request that is considered "urgent"?

Country	Channels, means and methods (Q 3.1.2)	Urgent requests (Q 3.1.3-3.1.5)
1. Albania	*Channel*: Usually the Ministry of Justice. *Means and methods*: Fax, email or in written form.	*Criteria*: Any indication of urgency; urgency specified in the request (e.g. imminent danger for life and health of people; substantial material damage) *Use of specific mechanisms, procedures or channels* As a requesting State, use of the most efficient channel available (foreign 24/7 contact point; direct communication by email or fax.) As a requested State, urgent requests have priority; direct contact by phone or email).
2. Armenia	*Channel*: General Prosecutor's office of RA *Means and methods*: e-mail, fax, phone	An indication of urgency: "urgent" status mentioned on request.
3. Australia	*Channel*: Diplomatic channels. *Means and methods*: Hard copy mutual assistance by diplomatic bag, courier and registered mail; Soft copies are also sent by email (where contacts are already established in the foreign country).	*Criteria*: Depending on the facts of a particular matter (e.g. pressing court or investigative timeframes; nature of the offence). *Use of specific mechanisms, procedures or channels* As a requesting State: Contacting the foreign authorities to alert them of a forthcoming

Country	Channels, means and methods (Q 3.1.2)	Urgent requests (Q 3.1.3-3.1.5)
		urgent request and provide brief details of its content; Sending a soft copy of the request (generally by email) signed by the Attorney-General's delegate. Using the federal police international liaison network to ensure reception of request and quick reaction. As a requested State: Provided sufficient information is given, contacting LEA to alert them and put the necessary preparations in place, pending the request.
4. Austria	*Channel*: N/a. *Means and methods*: Any means allowing for fast transmission, especially fax and e-mail.	*Criteria*: Danger of loss of data (in view of the short storage period in certain countries); data used as basis to carry out further investigative steps (e.g. freezing evidence). *Use of specific mechanisms, procedures or channels* Within the EU, Eurojust and European Judicial Network (EJN); Direct contact between judicial authorities.
5. Azerbaijan	All channels are acceptable.	
6. Belgium	All channels are acceptable.	*Criteria:* - Risk of live or physical injury - Imminent attacks on critical infrastructure Channels: police cooperation and direct contacts.
7. Bosnia and Herzegovina	*Channels*: Ministry of Justice (or Ministry of Foreign Affairs, where applicable) Bilateral international Agreements with Serbia, Croatia, Montenegro, Macedonia and Slovenia (criminal matters). And agreements assumed by succession INTERPOL; Eurojust; 24/7 contact points *Means and methods*: Telephone and email.	*Criteria*: Criminal offences which may have serious consequences (e.g. terrorism, murder, kidnapping); life-threatening situations; reasons to fear the alteration or destruction of digital evidence; other requests marked as 'urgent'. *Use of specific mechanisms, procedures or channels* INTERPOL, when provided by treaty.
8. Bulgaria	*Channel*: Legal assistance through competent authorities (and police cooperation through Europol, Interpol, liaison officers and	*Criteria*: When marked as urgent by the requesting State.

Country	Channels, means and methods (Q 3.1.2)	Urgent requests (Q 3.1.3-3.1.5)
	SELEC Centre). *Means and methods*: Ordinary mail, fax and email. National authorities may request the certification of authenticity of the material sent and the transmission of the originals.	*Use of specific mechanisms, procedures or channels* Possibility of using Interpol channel, as well as the European Judicial Network, Eurojust, consular officials, and liaison officers at the embassies.
9. Costa Rica	*Means and methods*: Various means of communication, especially scanned information sent via email, fax and courier when the request is urgent.	*Criteria*: Marking of the request as "urgent" by the requesting State, taking into account the merits of the particular case (type of offence; characteristics of victims and their involvement; etc.) *Use of specific mechanisms*, *procedures or channels*: As a requesting State, use of preliminary mechanisms to contact the requested State (including sending request via email) and obtain information on its requirements. As a requested State, national authorities seek a fast processing of documents (sending of digital copies of documents; use of courier to respond to request).
10. Croatia	*Channels*: Interpol. *Means and methods*: Letter, fax, email.	*Criteria*: Any request regarding a cybercrime offence. *Use of specific mechanisms, procedures or channels*: As a requesting State: No. As a requested State: No.
11. Cyprus	*Means and methods*: By fax, email, post, and in urgent cases through Interpol /Europol channels	*Criteria:* In the case that the investigation is on such a stage that there is a need to secure the stored data in order to conclude the investigation, as well as in the case that the investigation has been completed and the case is tried before the Court, therefore the computer data are needed to be presented as evidence before the Court. *Use of specific mechanisms, procedures or channels*: No. However, depending on the urgency of the case the channels of European Judicial Network and Eurojust may be used.
12. Dominican Republic	*Channel:* General Prosecutor of the Republic	Liaison officers represented in the country may be requested (FBI, Secret Service).

Country	Channels, means and methods (Q 3.1.2)	Urgent requests (Q 3.1.3-3.1.5)
13. Estonia	*Means and methods*: Usually emails (encrypted when necessary).	*Criteria*: Case-to-case approach. Main grounds: data retention, ongoing commission of a crime or prevention of an impending crime; prevention of financial loss; life protection; request marked as 'urgent' *Use of specific mechanisms, procedures or channels* Marking of the request as 'urgent'. Use of 24/7 networks and/or data communication systems of Interpol and Europol.
14. Finland	*Channels*: Diplomatic channels, direct contact, Interpol and Europol. *Means and methods*: Fax, email, regular mail.	*Criteria*: If a person has been arrested during the investigation and is kept in custody in this context; severe threat or danger to life, severe damage to property or environment, etc. *Use of specific mechanisms, procedures or channels* As a requesting State: See Q 3.1.2. Expedited execution is requested. As a requested State: Recourse to expedited execution and Eurojust 24/7 scheme.
15. France	*Means and methods*: Email (through a specific email box)	*Criteria*: Ongoing custody, important risk that data may be altered or deleted. *Use of specific mechanisms, procedures or channels* As a requested/requesting State: 24/7 contact point channel, where available.
16. Georgia	*Channels*: Channels established by international agreements, diplomatic channels, and other direct channels. *Means and methods*: Written form is favoured for validity purposes. Fax, email, or other methods are allowed.	*Criteria*: Case-by-case examination, based on the reasonable motivation of the urgency by the requesting State (especially short time-limits of judicial proceedings in the latter State). *Use of specific mechanisms, procedures or channels* As a requesting State: Labelling of the request as 'urgent'. The MoJ provided the reasoning for such label and can send scanned copy of the MLA request via email. As a requested State: Expedited initiation of all measures needed for executing the request; labelling of the request as 'urgent' in contacting domestic LEA; prompt information of the requesting State

Country	Channels, means and methods (Q 3.1.2)	Urgent requests (Q 3.1.3-3.1.5)
		when execution cannot be performed in the preferred time period.
17. Germany	*Means and methods*: Courier or email, depending on the urgency	*Criteria*: Ongoing custody, impending expiry of limitation period, risk of loss of data (expiry of the time limit for provisional preservation of data), risk to life and limb. *Use of specific mechanisms, procedures or channels* Transmitting the request in advance by email.
18. Hungary	*Means and methods:* E-mail, fax.	Same methods are used in general, but as a requested State make arrangements to obtain data immediately.
19. Iceland	Email and fax is sufficient to start execution of request and save time. However, the originals must follow shortly via mail	Depends on the specific case. For example, requests concerning imminent danger for life and health of people or substantial material damage, will always be prioritised. Also pressing court or investigative timeframes or the nature of the offence. As a requested state: The request gets prioritised at all fronts (Ministry, DPP and Police level).
20. Italy	It depends on the procedures commonly accepted by the requested State.	*Criteria*: When necessary to stop an ongoing crime. *Use of specific mechanisms, procedures or channels* No.
21. Japan	*Channels*: Central authorities pursuant to MLA treaties. *Means and methods*: International mail (EMS).	*Criteria*: N/a. No use of specific mechanisms, procedures or channels. Note: As a requested State, requests must be addressed to the central authorities for reasons of efficiency.
22. Latvia	*Channels*: State police and Prosecutor General's Office. *Means and methods*: Ordinary letter.	*Criteria*: The request relates to volatile data. *Use of specific mechanisms, procedures or channels* As a requesting/requested State: Direct contact and use of liaison officers' channels to duplicate and facilitate the request's execution.
23. Lithuania	*Channels*: The channel established in the prosecutor's office. *Means and methods*: Emails.	*Criteria*: No specific criteria. Issue examined on a case-to-case basis. *Use of specific mechanisms, procedures or channels*

Country	Channels, means and methods (Q 3.1.2)	Urgent requests (Q 3.1.3-3.1.5)
		The 24/7 network.
24. Moldova	*Channels*: The channel established in the prosecutor's office. *Means and methods*: Emails.	*Criteria*: Real danger that the evidence may be lost or destroyed; possible commission of further offences. Criteria are used to determine the reasonable time to solve the case (complexity of the case, conduction of proceedings, importance of the process for the person concerned, minority of the victim, etc.)
25. Montenegro	Lack of experience.	*Criteria*: N/a. *Use of specific mechanisms, procedures or channels* N/a.
26. Netherlands	*Channels*: Dependent on the priority given to the request. *Means and methods*: E-mail and telephone.	*Criteria*: Dependent on the request; vital interests or personal interest must be concerned. *Use of specific mechanisms, procedures or channels* Use of the telephone, and sometimes a meeting in person. Contact through the channel of the Single Point of Contacts.
27. Norway	Email to the relevant point of contact (as a starting point).	*Criteria*: Severity of the offence, possibility of losing vital evidence, possible loss of life (e.g. bomb threat). *Use of specific mechanisms, procedures or channels* As a requesting State: Yes and no. Use of the habitual channels, but followed-up with contact by phone. As a requested State: Yes. Possibility for prosecutors to issue a search or production order without a previous court approval. Detailed information on the degree of urgency (deadline, etc.) is welcomed.
28. Philippines	*Channels:* All communication system is allowed provided there will be subsequent transmittal of official request letter through diplomatic channels.	The criteria to consider a request as "urgent" and the procedures would depend on the particular Bilateral Agreement on MLA between the Philippines and the particular country.
29. Portugal	*Channels*: N/a.	*Criteria*: Ongoing detention or imprisonment, or issue related the

Country	Channels, means and methods (Q 3.1.2)	Urgent requests (Q 3.1.3-3.1.5)
	Means and methods: All communication systems, with priority given to email.	freedom of persons; cases marked as urgent by the proper authority; acts relating to the granting of parole. *Use of specific mechanisms, procedures or channels* As a requesting State: 24/7 contact points channel, as well as channels of the Interpol-G8 National Central Reference Points. As a requested State: Use of G8 channels.
30. Romania	*Channels*: Directly to the requested judicial authority, or through the central authority (depending on the applicable instrument). The Eurojust national officer is contacted to facilitate the execution of the request. *Means and methods*: Sending by post in all cases. Fax and email are used to speed-up the process.	*Criteria*: The person is under provisional arrest or investigations are to be carried out; a European Arrest Warrant is to be issued; time limit set for data retention (six months); risk of corruption and disappearance of the digital evidence. *Use of specific mechanisms, procedures or channels* As a requesting State: Sending of requests by fax and email. Direct contact, where possible, with the person executing the request. Specification of applicable deadline and of the fact that the defendant is under provisional arrest. Involvement of the Eurojust national officer. As a requested State: Priority is given to the execution of the request. When participating to the execution, the requesting authorities may receive directly copies of documents and evidence seized
31. Serbia	*Channels*: Usually through the Ministry of Justice. *Means and methods*: N/a.	*Criteria*: Any indication of urgency; urgency specified in the request (e.g. imminent danger for life and health of people; substantial material damage). *Use of specific mechanisms, procedures or channels* As a requesting State, use of the most efficient channel available (foreign 24/7 contact point; direct communication by email or fax.) As a requested State, urgent requests have priority; direct contact by phone or email).
32. Slovakia	In non-urgent cases the regular mail is used. In urgent cases requests may be sent through Interpol, by fax, e-mail, subject to	Requests under Article 29 are urgent (taking into account the aim of making data available for consequent MLA request and the possible

Country	Channels, means and methods (Q 3.1.2)	Urgent requests (Q 3.1.3-3.1.5)
	conditions of applicable international treaty.	risk of loss of data). No internal rules were prescribed/elaborated in order to consider the MLA request "urgent". Of course, a deadline for preservation may justify the urgency of a request. In general, the assessment of a request is made on case-by-case basis. The urgency of a request is either determined by the possibility of a loss of data (e.g. a period for a storage of data may expire soon) or by a severity of the offence or by an impact of data on the criminal case or by a simple fact that an accused in detained etc. As a requesting State: In a case of urgent request, a modern means of communication or a transmission of a request may be used. In such cases a direct communication with counterparts may be applicable as well in order to make sure that everything will happen in time. The use of Interpol and other secure channels is also considered. As a requested State: The mechanisms, procedures or channels are mainly determined by the requesting state. Therefore as a requested state we may consider different options only if there is a need for additional information and further communication. All available means may be used.
33. Slovenia	*Channels*: Usually, Interpol and Europol channels. *Means and methods*: N/a.	*Criteria*: Life-threatening situation, national security, public threat of high level. *Use of specific mechanisms, procedures or channels* As a requesting State: Use of the 24/7 contact points provided for by the Cybercrime Convention. As a requested State: Lack of sufficient experience.
34. Spain	*Means and methods*: Usually by post.	*Criteria*: Time elapsed since the facts (issues of deletion of data, time limitation of the offence), importance of the crime investigated, the

Country	Channels, means and methods (Q 3.1.2)	Urgent requests (Q 3.1.3-3.1.5)
		marking of the request as 'urgent' by the requesting State, etc. *Use of specific mechanisms, procedures or channels* As a requesting State: Preliminary sending of the request by email and/or fax; use of contact points of EJN, IbeRed, and its communication system Iber@. As a requested State: Priority is given to urgent requests; liaison with the requesting State.
35. Switzerland	*Channels*: Interpol, Europol channels for police cooperation; diplomatic channels for regular mails. *Means and methods*: Fax, e-mail, followed by a formal request in writing. Secured mailboxes are often used (e.g. Europol's SIENA)	*Criteria*: Imminent danger that data could be lost/deleted; a reply is expected within 24 hours (Interpol's standard). *Use of specific mechanisms, procedures or channels* MLA: No. Police cooperation: (Requesting) Possibility to mark the request as 'urgent' and inform competent authorities informally – email, phone. (Requested) Priority is given to urgent requests.
36. "The former Yugoslav Republic of Macedonia"	*Channels*: Agreement with Serbia, Croatia, Montenegro and Bosnia-Herzegovina on organised crime and corruption cases (and other criminal matters). Under certain conditions, direct contact between prosecutors is possible. *Means and methods*: Mostly emails.	*Criteria*: Requests asking for a reply within 24 hours. *Use of specific mechanisms, procedures or channels* As a requesting State: No specific mechanisms; the request is marked as 'urgent'. As a requested State: No specific mechanisms.
37. Turkey	*Channels*: Ministry of Justice. *Means and methods*: Written form, fax and emails.	*Criteria*: Serious crimes, life-threatening situations, preservation term. *Use of specific mechanisms, procedures or channels* As a requesting State: use of INTERPOL and 24/7 contact points, by fax, email or phone. As a requested State: Use of contact/point mechanism, by fax, email or phone.
38. Ukraine	(MoI)	(MoI)

Country	Channels, means and methods (Q 3.1.2)	Urgent requests (Q 3.1.3-3.1.5)
	Channels: Diplomatic channels. *Means and methods*: Phone, email. (Sec Serv) *Means and methods*: Only by post, according to national law.	*Criteria*: Request aiming at the preservation of data that can be used as electronic evidence, since data is very volatile. *Use of specific mechanisms, procedures or channels* No. (Sec Serv) *Criteria*: No criteria. Dependent on the specific situation and request. *Use of specific mechanisms, procedures or channels* As a requesting State: As a requested State: Possible, as an exception, to receive requests by email, fax, etc., before official reception by post
39. United Kingdom	*Means and methods*: Usually by post, unless secure fax or email facilities exist.	*Criteria*: Cases where a person is in custody or due to be released from custody; immediate risk to individuals; risk of dissipation of assets. *Use of specific mechanisms, procedures or channels* As a requesting State: Labelling of the request as 'urgent', justifying the use of such label and giving additional information. As a requested State: The central authority deals with the request as quickly as possible. Specific requirements apply (justification of the urgency, deadlines, follow-up where assistance is no longer needed).
40. United States of America	*Channels*: Central authorities (In case of preservation, central authorities' channels or 24/7 network). *Means and methods*: Expedited means, including fax or email.	*Criteria*: Threats to life or of physical injury; threats to important infrastructures; cases involving children; significant danger of continued criminality, destruction of data or flight of a suspect, forthcoming arrest or impending trial. *Use of specific mechanisms, procedures or channels* Extensive use of 24/7 channels. Transmission of requests electronically, or before the completion of its translation (where agreed with the requested State). Close telephone or email contacts. Note: Electronic transmission of requests is not limited to urgent cases

4.6.3 Role of 24/7 point of contact (Question 3.2)

3.2 Role of 24/7 contact points with respect to mutual assistance (relationship between Article 35 and Article 31 Budapest Convention) 3.2.1 Does your 24/7 contact point have the competence to send or receive requests for mutual assistance? If yes, please explain the role of the 24/7 contact point, including in the executing of a request. 3.2.2 If the 24/7 contact point does not itself have competence for mutual assistance, please explain how 24/7 contact points coordinate with the competent authorities for mutual assistance on an expedited basis (Article 35.2b). Please describe the relationship between the two offices and how cooperation may be improved to expedite the execution of requests for mutual assistance.

Country	Competence for MLA requests (Q 3.2.1)	Coordination with MLA authorities (Q 3.2.2)
1. Albania	*Competence*: Yes. *Role*: To send and receive requests, communicates, exchanges data and legal advices with other CPs. The CP communicates with ISPs and other legal persons and transmits directly the data obtained.	*Improvements*: Replacement of the letter rogatory by electronic requests; possibility for CPs to send/receive directly a request, with a notification to the relevant Ministry of Justice.
2. Armenia	*Competence*: No. The competence MLA requests is with the General Prosecutor's Department *Role*: 24/7 contact point may only execute requests not requirement MLA.	If a request is "urgent" it can be sent via 24/7 contact point, but an official MLA request will be required to obtain requested information. In case the 24/7 CP at the police initiates a request requiring MLA, the police appeals to General Prosecutor's office.
3. Australia	*Competence*: No. But the point of contact can provide police-to-police assistance to foreign countries a pending formal request.	Good working relationship and regular liaison regarding mutual assistance requests.
4. Austria	*Competence*: No. But the point of contact is an intermediary with the prosecution services and can transmit request to the domestic competent authority.	Direct and informal communication between the 24/7 contact point and the executing authorities. No delay caused by this coordination.
5. Azerbaijan	*Competence:* Yes. The contact point can provide specialised assistance, order the expeditious preservation of computer data or traffic data, after getting court decision the seizure of objects containing data and perform or facilitate the execution of procedural	

Country	Competence for MLA requests (Q 3.2.1)	Coordination with MLA authorities (Q 3.2.2)
	documents.	
6. Belgium	No.	Such procedures are not yet in place.
7. Bosnia and Herzegovina	*Competence*: Yes, through Interpol channels *Role*: To transmit mutual assistance in urgent cases.	N/a.
8. Bulgaria	*Competence*: No.	Very good cooperation with the MLA authorities, made necessary by the fact that the contact point is the only specialised unit in cybercrime in the country. If the MLA authority forwards a request to the contact point, the latter can ensure the preservation and obtaining of electronic evidence.
9. Costa Rica	*Competence*: Yes. The contact point is in charge of proceedings regarding international criminal cooperation and is a central authority for various international instruments on mutual assistance.	Not applicable.
10. Croatia	*Competence*: No.	The CP sends the request to the competent unit, which makes verifications. The necessary criminal investigation conducted is coordinated with the competent State attorney.
11. Cyprus	Yes. The contact point which is the Head of Cybercrime Unit can accept MLAs and he has the supervision of their execution. He is also responsible to inform the MJPO.	Not applicable.
12. Estonia	*Competence*: Yes, but only to send and receive requests.	The 24/7 contact point: has competence to forward information to the relevant units and to find a competent recipient, who can provide his/her expertise even outside working hours when needed; ensures that information is transmitted to the competent decision maker.
13. Finland	*Competence*: Yes, according to section 5 of the MLA law. *Role*: The contact point can make an MLA request and participate in the execution of requests. According to general MLA law section 5, MLA request can be made by Ministry of Justice, court, prosecutor or investigative authority	N/a. See Q 2.1. If the authority is not competent, it has an obligation to transmit it to competent authority.

Country	Competence for MLA requests (Q 3.2.1)	Coordination with MLA authorities (Q 3.2.2)
	(e.g. police). Our 24/7 contact point is a police authority (in NBI). According to section 4 of the general MLA law MLA requests to Finland can be made to Ministry of Justice or directly to such authority which is competent to execute the request. Police has wide role and competence in executing MLA requests in Finland when acting as investigative authority.	
14. France	*Competence*: No.	As regards data freezing, interaction between the Ministry of Justice (Bureau d'entraide pénale internationale) and the 24/7 point of contact within the Ministry of Interior. No information on whether requests made via the 24/7 network of contact points are then subject to mutual assistance requests.
15. Georgia	*Competence*: Yes. The 24/7 contact point can send/receive requests and undertake all necessary measures to provide assistance. Where a request falls beyond its competence, it addresses the request to the Ministry of Justice.	N/a. See Q 3.2.1.
16. Germany	*Competence*: No. But the 24/7 contact point can arrange for advanced preservation of data.	*Incoming* requests: The 24/7 contact point may arrange the provisional preservation of data; upon reception of the request, it may initiate initial contact with the Federal Office of Justice. *Outgoing* requests: Contact by the competent LEA with the 24/7 contact point, either in advance, or at the initiative of the FOJ once the request has been received.
17. Hungary	24/7 contact point is authorised to send/receive MLA requests (transmission role)	Not applicable.
18. Iceland	No. All requests are forwarded to the Ministry.	The 24/7 contact point contacts the responsible Legal Expert at the Ministry.
19. Italy	[to be clarified]	N/a.
20. Japan	*Competence*: No.	Liaison of the 24/7 contact point with the competent central authority, through emails and phone calls where necessary.
21. Latvia	*Competence*: The 24/7 CP sends/receives, exchanges data and	Direct contacts between State police and the Prosecutor General's Office.

Country	Competence for MLA requests (Q 3.2.1)	Coordination with MLA authorities (Q 3.2.2)
	follows up to requests for preservation of data. CP has the powers of intelligence institution (CP could verify any kind of data or CP can forward a request to competent institution if the subjects of request or the actions are sophisticated.	
22. Lithuania	*Competence*: Yes. The 24/7 contact point can directly send/receive, execute and follow up to requests for preservation of data.	Not applicable (See Q 3.2.1)
23. Moldova	*Competence*: No.	Activities of the prosecutors, investigators and officers involved in cybercrimes cases within the same building; Use of methods of urgent communication.
24. Montenegro	*Competence*: Yes. *Role*: To send and receive MLA requests.	N/a.
25. Netherlands	*Competence*: Yes, the 24/7 contact point can send/receive MLA requests; this channel is rarely used. In urgent matters, the 24/7 network may be used to receive requests in advance.	Preparation of the request by the high-tech crime team, which sends the draft the NPO. The NPO finalises the request and a prosecutor signs it.
26. Norway	*Competence*: Yes. The point of contacts has police officers, prosecutors and Interpol and Europol contact points. Location of the National Authority for Prosecution in the same building.	Not applicable.
27. Philippines	Only through the Department of Justice.	The DOJ is the competent authority with regard to requests for mutual legal assistance.
28. Portugal	*Competence*: No.	The contact point has the legal competence to execute urgent requests for preservation of data. It transmits immediately formal requests as well as other measures beyond its competence to the Public Prosecution Service, for their expedited implementation.
29. Romania	*Competence*: Yes. The contact point can provide specialised assistance, order the expeditious preservation of computer data or traffic data, and the seizure of objects containing data and perform or facilitate the execution of letter rogatories.	Direct cooperation between the point of contact and the Office for international cooperation within DIICOT or other domestic prosecution offices;
30. Serbia	*Competence*: Yes. *Role*:	*Improvements*: Replacement of the letter rogatory by electronic

Country	Competence for MLA requests (Q 3.2.1)	Coordination with MLA authorities (Q 3.2.2)
	To send and receive requests, communicate, exchange data and legal advice with other CPs; To communicate with ISPs and other legal persons and transmit directly the data obtained.	requests; possibility for CPs to send/receive directly a request, with a notification to the relevant Ministry of Justice.
31. Slovakia	24/7 contact point is the National Bureau of Interpol. It is the channel, which may facilitate transmission of a request.	National Interpol Bureau is in direct contact with the General Prosecutor´s Office. The prosecution service is hierarchically organized. In the Slovak Republic, a system of prosecutors on duty (24/7) is applied.
32. Slovenia	*Competence*: Yes. 24/7 contact points receive requests from all police units, translate requests and send them to the requesting State; 24/7 contact points receive foreign requests and send them to the competent police unit.	Not applicable.
33. Spain	*Competence*: Yes. It has competence for measures of execution only in cases of police cooperation.	No answer available.
34. Switzerland	N/a.	N/a.
35. "The former Yugoslav Republic of Macedonia"	*Competence*: Yes. *Role*: To send and receive requests. As a public prosecutor, the CP can: directly communicate with the investigating judge for the issuance of a freezing or seizure order; and communicate through the MoJ for further mutual assistance.	N/a.
36. Turkey	*Competence*: No.	The CP submits the request to the MLA central authority (the Ministry of Justice) to start investigations in Turkey, or to obtain the execution of the request via a prosecutor or court order.
37. Ukraine	(MoI) *Competence*: No. (Sec Serv) *Competence*: No.	(MoI) The contact point does not take part to the execution of mutual assistance requests. (Sec Serv) The 24/7 contact point can only exchange operative information;

Country	Competence for MLA requests (Q 3.2.1)	Coordination with MLA authorities (Q 3.2.2)
		Absence of specific mechanism to share information on cybercrime between relevant agencies.
38. United Kingdom	*Competence*: Yes.	Not applicable.
39. United States of America	*Competence*: No. (But forward requests to the central authority to facilitate cooperation and assist the central authority as necessary)	Notification by the contact point of 24/7 requests to the central authority. Possibility for the 24/7 contact point to assist the central authority in handling difficult, large or urgent case.

4.6.4 Direct contact to obtain data from physical or legal persons (Question 3.3)

3.3 Direct contact to obtain data from legal or physical persons 3.3.1 Does your domestic law allow you to contact holders of data (such as Internet service providers) in foreign jurisdictions directly to obtain stored data? If yes: What are the conditions? For what type of holders of data (ISPs, other private sector entities, physical persons)? Does the type of data (subscriber, traffic, content) requested make a difference? 3.3.2 Does your domestic law allow foreign law enforcement to contact directly holders of data located in your State? If yes: What are the conditions? For what type of holders of data (ISPs, other private sector entities, physical persons)? Does the type of data (subscriber, traffic, content) requested make a difference? 3.3.3 If no, what are the sanctions?

Country	Direct contact of domestic LEA to physical/legal persons in foreign jurisdiction (Q 3.3.1)	Direct contact of foreign LEA within national jurisdiction (Q 3.3.2 – 3.3.3)
1. Albania	Prosecutor: Direct contact by the prosecutor is allowed, for any type of holder of data. Judicial police officers: Direct contact is allowed, but only to obtain subscriber information. A possible solution will be to request the data to the local representative of the ISP.	No explicit prohibition under domestic law. A court order is required for content data. Sanction (where domestic preconditions are not fulfilled): The contact qualifies as an offence.
2. Armenia	The law does not prevent such contacts, although the execution of a request depends on ISPs or entity requested.	It is possible under the law but the response depends on the ISP or entity.
3. Australia	No specific legal basis under national law. In practice, data is sought by way of a mutual assistance request. In practice, this may occur if agency is aware that the applicable national law for the ISP would allow direct request, otherwise data is sought by	No legal basis under national law. Such action is limited under national law (carriers of data can be compelled to release material only in certain cases). Sanction (for the holder of the data): Offence punished by up to 2 years of

Country	Direct contact of domestic LEA to physical/legal persons in foreign jurisdiction (Q 3.3.1)	Direct contact of foreign LEA within national jurisdiction (Q 3.3.2 – 3.3.3)
	way of a mutual assistance request.	imprisonment.
4. Austria	Not legally allowed in principle. In practice, direct contact to avoid deletion of data was made only with ISPs located in the USA (as asked by US authorities themselves), with positive effects.	No legal basis. Sanction: Conduct qualifies as an infringement of State sovereignty.
5. Azerbaijan	Direct contact is usually used to obtain subscriber information.	
6. Belgium	It is possible to contact ISPs directly if there is an agreement with a provider (e.g. with Google, Microsoft, Facebook). This only applies to subscriber and traffic data. For content judicial cooperation is necessary.	No. If the procedure is illegal, the results obtained cannot be used in proceedings.
7. Bosnia and Herzegovina	No clear legal basis. Direct contact is possible in practice, in urgent cases; an official request must be sent later on.	Possible in practice.
8. Bulgaria	No clear legal basis under national law.	No legal framework. Pursuant to national law, legal and physical persons may be obliged to provide information, or may be able to refuse to do so. Content data can be provided if it comes from or affect specific natural or legal person, with his consent.
9. Costa Rica	N/a. General remark: Domestic law does not allow for the application of any foreign law.	N/a. See Q 3.3.1
10. Croatia	No legal basis. In practice: Possible, on the basis of the Cybercrime Convention.	In principle: Not possible. Sanction: Refusal of the request. In practice: Possible, on the basis of the Cybercrime Convention.
11. Cyprus	Not possible	Not possible MLA procedure required.
12. Estonia	Not regulated in national law. In practice, domestic authorities do contact foreign ISPs.	Not regulated in national law. Yet, certain data holders including ISPs can only disclose data to domestic authorities. Sanction: Violation of national law entailing administrative proceedings.
13. Finland	Not regulated in national law. May fall under the criminal offence of violation of official duty by a public officer.	See Q 3.3.1.
14. France	Not regulated in national law.	No legal basis.

Country	Direct contact of domestic LEA to physical/legal persons in foreign jurisdiction (Q 3.3.1)	Direct contact of foreign LEA within national jurisdiction (Q 3.3.2 – 3.3.3)
	In practice, judicial requests are addressed to ISPs in a foreign jurisdiction (e.g. Facebook, Google) to identify users, where the ISP does not have a local office or is overburdened by requests.	Absence of known practice.
15. Georgia	Not regulated in national law. In practice, it is possible to obtain data from ISPs and other private entities located abroad, with their voluntary consent. Such data can be used as evidence in court.	Not regulated in national law. Sanction: Dependent on the type of data sent without the permission of domestic authorities (sending of secret information entails criminal liability; sending other information is subject to administrative sanctions).
16. Germany	Yes, provided contact is undertaken by the prosecution authorities and does not involve enforcement measures.	No. Sanction: N/a.
17. Hungary	Not possible.	Not possible. No sanctions foreseen.
18. Iceland	No.	No. Not regulated in Icelandic law.
19. Italy	Not allowed under domestic law.	No. Sanction: N/a.
20. Japan	No clear prohibition under domestic law, but direct contact without prior approval of the concerned State would amount to an infringement of State sovereignty.	No, pursuant to international law (State sovereignty); ISPs within national jurisdiction are not allowed to disclose information falling under secrecy of communication to foreign LEA. Exception: Necessity; issuance of a court order. Sanction: Determined on a case-by-case basis.
21. Latvia	No. Direct contact cannot be used to obtain evidence.	No. Sanction: Dependent on the type of data. It can reach criminal liability for illegal disclosure of content data/correspondence.
22. Lithuania	No prohibition under national law, but certain requirements must be met. In practice: Direct contact is usually used to obtain subscriber information, as well as traffic and content data.	No prohibition under national law, but the applicable domestic limits and prohibitions shall be respected (e.g. information related to State secrets, privacy and private life, etc.). Sanction: Depending on the type of offence, the sanction may be of a fine or a term of imprisonment of two to fifteen years.
23. Malta	Domestic law does not allow or disallow local law enforcement to contact service providers that are located overseas.	Domestic law does not allow or disallow foreign law enforcement to contact service providers that are located locally. The Malta Police Force is not aware of any such requests.

Country	Direct contact of domestic LEA to physical/legal persons in foreign jurisdiction (Q 3.3.1)	Direct contact of foreign LEA within national jurisdiction (Q 3.3.2 – 3.3.3)
	In a number of cases, foreign services providers have been requested to provide subscriber and traffic data directly to the Malta Police Force. Whether or not the requested information is provided directly to local law enforcement varies according to the contacted service provider. Content data has never been requested directly from foreign service providers.	As a general rule, attempts are first made to obtain information directly from the service providers. Requests for information are followed through police channels or mutual assistance if direct correspondence is unsuccessful.
24. Moldova	No.	No. Considered as a breach of sovereignty. Sanction: Cancellation of illegally obtained evidence.
25. Montenegro	No legal basis and lack of experience. Direct contact is legally possible, but there is no guarantee that the evidence will be accepted in court.	Direct contact is possible in practice.
26. Netherlands	No legal prohibition under domestic law. Respect of the national law of the State concerned.	No.
27. Norway	Not regulated in national law. In practice: Direct contact is limited to specific ISPs, mainly to obtain subscriber information or to freeze data pending a formal request.	No, regarding customer information and logs (duty of secrecy); Yes, regarding subscriber information, as well as other type of data if the ISP agrees to such delivery. Sanction (In case of violation of the Data Protection Act by a domestic ISP): Fines or prison sentences. No practice.
28. Philippines	There were attempts to directly contact ISP's in foreign jurisdiction but only accommodated for preservation and not for production of data, including subscriber information.	No. Sanction possible under Republic Act No. 10173 or the Data Privacy Act of 2012, and Republic Act No. 10175 or the Cybercrime Prevention Act of 2012.
29. Portugal	Yes (for any data), in situations where (a) the data is publicly available, or (b) there is a legal and voluntary consent of the person legally authorised to disclose the data. Such action can be subject to certain requirements (in particular, the issuance of a judicial order).	Yes (for any data), in the same situations as described in Q 3.3.1.
30. Romania	Yes, pursuant to arrangements allowing obtaining directly subscriber information and logs from Google and Facebook. The data obtained cannot be used as evidence without a subsequent mutual assistance request.	No, for reasons of national sovereignty; exception provided by the implementation of art.32 b CCC Sanction: N/a.

Country	Direct contact of domestic LEA to physical/legal persons in foreign jurisdiction (Q 3.3.1)	Direct contact of foreign LEA within national jurisdiction (Q 3.3.2 – 3.3.3)
31. Serbia	No legal obstacles in domestic law. Prosecutor: Direct contact by the prosecutor is allowed, for any type of holder of data and any data. Judicial police officers: Direct contact is allowed, but only to obtain subscriber information. E.g. Unsuccessful direct contact with Facebook a few years ago; other actions through Interpol channels.	No explicit prohibition under domestic law. A court order is required for content data. Sanction (where domestic preconditions are not fulfilled): The contact qualifies as an offence.
32. Slovakia	No. Although it is not strictly prohibited to request data from holders in foreign jurisdictions directly, the problem would be in use of such data as evidence. According to our legislation the evidence from abroad shall be requested via mutual legal assistance.	It is a complex issue. In principle, if no involvement of official authorities of the Slovak Republic is presumed and/or used, it would be possible to obtain such data from the Slovak Republic. However, we believe such possibility is highly hypothetical and applicable only in very simple cases. Data cannot be requested with any warning on the application of sanction or penalty, if the holder of data does not provide such data voluntarily. A number of data is, at the same time, protected through bank or telecommunication secrecy or through data protection legislation. Such data may be disclosed only under the conditions prescribed by the laws of the Slovak Republic. Therefore, as a matter of principle, data stored in Slovakia may be requested for the purposes of criminal proceedings only through application of mutual legal assistance. If there is any breach of telecommunication, bank or other secrecy, data protection rules, administrative or even criminal sanction may apply. It should be noted that legality principle is applied in the Slovak Republic. Negative consequences for admissibility of evidence obtained in a way described above may follow.
33. Slovenia	Not allowed under national law.	Not allowed under national law. Sanction: Various money penalties, as prescribed in electronic communication law.
34. Spain	No.	No. Sanction: No sanction as such. Lack of validity and admissibility of the evidence/data gathered, and lack of LEA powers to obtain data forcibly.
35. Switzerland	Not allowed under national law;	-Not allowed under national law;

Country	Direct contact of domestic LEA to physical/legal persons in foreign jurisdiction (Q 3.3.1)	Direct contact of foreign LEA within national jurisdiction (Q 3.3.2 – 3.3.3)
	Allowed under article 32.b of the Convention on Cybercrime.	Allowed under article 32.b of the Convention on Cybercrime. Sanction (When article 32.b is not applicable): Criminal offence, punishable by up to 3 years of imprisonment or a fine.
36. "The former Yugoslav Republic of Macedonia"	Direct contact is not prohibited, even though experience on direct contact concerns mostly Facebook.	No. [to be clarified]
37. Turkey	No explicit prohibition under domestic law. It may depend on the existence of relevant interstate agreements. In practice, data is regularly sought through direct contact. Data obtained without MLA request is unlikely to be accepted in proceedings, pursuant to a decision by the Turkish Supreme Court on the implementation of Law 2992.	As regards traffic data and content data, direct contact is not possible (need for a court order, or in case of peril, the public prosecutor's approval). Sanction: Data should not be accepted as evidence in court proceedings.
38. Ukraine	(MoI) No legal basis under national law. Direct contact is not used in practice. (Sec Serv) No legal basis under national law.	(MoI) No clear prohibition under national law, with some restrictions (law on protection of personal data; State secrecy). Sanction (when restrictions are not respected): Criminal liability. (Sec Serv) No legal basis under national law. Sanction (when restrictions are not respected): Criminal liability.
39. United Kingdom	Yes. The only conditions depend on those set by the requesting State.	Yes, if the lawful owner of the data chooses to do so. Sanction: None.
40. United States of America	Yes, if allowed by the foreign State and within the limit of what seems acceptable to this State.	Yes. Especially with ISPs, which may voluntarily agree to disclose traffic and subscriber data (content data cannot be directly disclosed); Also with other physical/legal persons, provided that national authorities are notified. Sanction: No practice. Possibly, refusal to assist the requesting State in obtaining formal copy of evidence usable in court.

4.6.5 Coordination in complex cases (Question 3.4)

Replies to the questionnaire referred to the following mechanisms to coordinate complex cases requiring concerted action (such as searches) in multiple States:

Country	Mechanisms for the coordination of complex cases
1. Albania	Usually under the framework of police organisations, such as INTERPOL.
2. Armenia	The high-tech crime division of the police is available to coordinate domestically in complex international cases
3. Australia	Upon reception of a request, liaison between the federal police with officers within the country and abroad (using an extensive international liaison officer network).
4. Austria	Coordination mechanisms provided by the central authority, as well as Eurojust and the contact points of the European Judicial Network.
5. Belgium	Joint investigation teams.
6. Bosnia and Herzegovina	MLA mechanisms.
7. Bulgaria	The Supreme Prosecution Office of Cassation can set up joint investigation teams with other States, composed of prosecutors and investigators. An agreement among the competent authorities of the participating states shall be agreed upon (activities, duration and composition of teams); Mutual legal assistance; Coordination with the liaison officers.
8. Costa Rica	National law allows joint research work between the Attorney General and various (foreign) State authorities.
9. Croatia	Joint investigation team on the basis of int.treaty (art. 201. of CPA) and via EUROJUST
10. Cyprus	n/a
11. Estonia	Involvement of different experts and specialists in case of need; Coordination of police forces all over the territory (following reception of a request by the liaison officers of the Bureau of Criminal Intelligence).
12. Finland	Ad-hoc approach, depending on the nature of the case.
13. France	Operational meetings on specific objectives, via Europol or Interpol.
14. Georgia	Joint crime detection teams, allowing for concerted action (e.g. searches).
15. Germany	Coordination of parallel requests (e.g. coordinated coercive measures) Eurojust, European Judicial Network, Joint Investigation Teams, direct communications between prosecutors
16. Hungary	n/a
17. Italy	Letters rogatory are the only mechanism enabling such coordination.
18. Japan	International cooperation through the ICPO network, diplomatic channels and central authorities competent under applicable MLA agreements.
19. Latvia	European Cybercrime Centre (EC3), Joint investigation teams; Liaison offices.
20. Lithuania	Joint investigation teams, including foreign officers when an agreement is in force.
21. Malta	
22. Moldova	Joint investigation teams, on the basis of State agreement.
23. Montenegro	N/a.
24. Netherlands	N/a.

Country	Mechanisms for the coordination of complex cases
25. Norway	No specific mechanisms; Assistance of Eurojust in certain cases.
26. Philippines	Intelligence sharing and cooperation with attaches of the foreign state and INTERPOL.
27. Portugal	Joint investigation teams, set up by State agreements.
28. Romania	Use of Eurojust network; Coordination of all national authorities involved; Involvement of the liaison magistrates and officers within accredited embassies; Creation of joint investigations teams.
29. Serbia	Usually under the framework of police organisations, such as EUROPOL and INTERPOL
30. Slovakia	The use of Europol/Eurojust may be considered as a working solution even with the countries outside of the European Union.
31. Slovenia	Lack of sufficient experience.
32. Spain	Use of Eurojust networks, where applicable; Coordination of investigative measures, through liaison with foreign judicial authorities
33. Switzerland	Coordination of all authorities involved by the Federal Office of Justice; Coordination of inter-cantonal and international investigation by the Federal Office of the Police (Fedpol).
34. "The former Yugoslav Republic of Macedonia"	Absence of specific mechanisms.
35. Turkey	Activities (meetings, seminars, joint projects, etc.) with counterparts to share knowledge and discuss problems; Signature of Protocols and understandings with foreign central authorities to further cooperation; Establishment of CP to facilitate communication between judicial authorities; Use of internationals channels (INTERPOL, SECI Center, EUROJUST and other), as well as cooperation with foreign financial intelligence units.
36. Ukraine	Ministry of Interior: Decided by each competent body. No strict provisions regulating this issue. Security Service: Joint (international) investigative teams set up by the General Prosecutor's Office.
37. United Kingdom	Use of Eurojust networks, or equivalent.
38. United States of America	Hard work, email, phone calls, meetings if necessary.

5 Conclusions and recommendations

As indicated at the outset: expeditious mutual legal assistance (MLA) is one of the most important conditions for effective measures against cybercrime and other offences involving electronic evidence given the transnational and volatile nature of electronic evidence. In practice, however, mutual legal assistance procedures are considered too complex, lengthy and resource intensive, and thus too inefficient.

The T-CY, therefore, carried out a detailed assessment of the functioning of mutual legal assistance with a focus on Article 31 Budapest Convention. The assessment was based on replies from 36 Parties and three Observer States. Discussions were held at the 9th Plenary (June 2013), 10th Plenary (December 2013), 11th Plenary (June 2014) [and 12th Plenary, December 2014. The present report was adopted in xxx]

This assessment and the solutions proposed by responding States result in the following conclusions and recommendations.

5.1 Conclusions

5.1.1 Overall conclusions

Concl 1 The mutual legal assistance (MLA) process is considered inefficient in general, and with respect to obtaining electronic evidence in particular. Response times to requests of six to 24 months appear to be the norm. Many requests and thus investigations are abandoned. This adversely affects the positive obligation of governments to protect society and individuals against cybercrime and other crime involving electronic evidence.

Concl 2 And yet, Parties appear not to make full use of the opportunities offered by the Budapest Convention on Cybercrime and other agreements for the purposes of effective mutual legal assistance related to cybercrime and electronic evidence.

Concl 3 Detailed data or statistics on MLA are not available. It may be useful to establish mechanisms to monitor the MLA process related to cybercrime and electronic evidence.

5.1.2 Frequency of requests and types of data requested

Concl 4 In terms of the type of data requested, subscriber information has been singled out as the most often sought information. The large amount of requests for such information puts a heavy burden on authorities responsible for processing and executing MLA requests and slows down and often prevents criminal investigations. This suggests that solutions to the challenge of subscriber information would render MLA more efficient.

Concl 5 MLA requests for electronic evidence seem most often related to fraud and financial crimes, followed by violent and serious crimes. Mutual assistance for accessing stored computer data is thus not only related to cybercrime (offences against and by means of computers (Articles 2 to 11 Budapest Convention), but comprises the collection of evidence in electronic form in relation to any criminal offence.

Concl 6 Police-to-police cooperation is much more frequent than MLA. Much information can be shared but often requires validation before use as evidence in court.

Concl 7 The opening of a domestic investigation upon receipt of an MLA request or spontaneous information may facilitate the sharing of information without MLA or accelerates MLA.

5.1.3 Procedures and requirements

Concl 8 The formal requirements and applicable legislation of the requested State are often not known or not met. Requests are often incomplete or too broad or do not meet legal thresholds or the dual criminality requirement. More training, more information on requirements to be met and standardised and multilingual templates for requests would be useful.

Concl 9 Some States may refuse cooperation if the case appears minor or puts an excessive burden on the requested State. More information and dialogue are required if thresholds apply.

Concl 10 The question of language of international requests for mutual assistance is a major problem, because of the delay and cost and because of the limited quality of translations. Most Parties accept requests in English.

5.1.4 Channels and means of cooperation

Concl 11 Most Parties make use of different bilateral, regional and multilateral agreements or the principle of reciprocity, and multiple authorities and channels of cooperation as foreseen in the Budapest Convention on Cybercrime. Some States, however, follow a more limited approach and require MLA requests to be sent via Ministries of Justice and a few only accept requests via diplomatic channels.

Concl 12 The possibility of direct cooperation with foreign judicial authorities appears to be underused – except between EU member States. This limited use of the option of direct cooperation also seems to be the case for non-EU States that are nevertheless Parties to the 2nd Additional Protocol to the Convention on Mutual Legal Assistance in Criminal Matters (ETS 182) of the Council of Europe. It may be worth considering provisions allowing for direct cooperation between Parties to the Budapest Convention.

Concl 13 States follow different approaches for considering requests as "urgent". A significant number of Parties treat a request as urgent if there is a risk of loss or modification of data. In such cases, use is made of 24/7 points of contact, liaison officers, judicial networks or police-to-police cooperation. However, it appears that requests are not always "responded to on an expedited basis" as foreseen in Article 31.3 Budapest Convention.

Concl 14 Under Article 35, 24/7 points of contact, if they are not themselves able to engage in mutual legal assistance, should be able to coordinate with authorities responsible for MLA on an expedited basis. While some – in particular prosecution-type – contact points can send, receive and execute requests and while others can transmit requests, overall the actual role of 24/7 contact points in MLA appears to be too limited.

Concl 15 The prosecution or police services of many States contact foreign service providers directly, in particular those based in the United States, and these may respond positively under certain conditions. Such requests may take the form of domestic production orders. Some providers may respond directly to requests related to emergency situations. Overall, conditions for such direct contacts are unclear; in some

countries information thus obtained may need to be validated through a subsequent MLA request before use as evidence in court.

Concl 16 The setting up of joint investigative teams may facilitate coordination in complex cases. JITs may be set up subject to bi- or multilateral agreements in force. The Budapest Convention, at present, does not specifically provide for such a mechanism.

5.2 Recommendations

These recommendations point at actions to be taken by Parties domestically and/or the T-CY and capacity building programmes.

Some recommendations may need to be addressed through an Additional Protocol. However, the present report and its recommendations shall not pre-empt a decision on the preparation of a Protocol.

5.2.1 Recommendations[24] falling primarily under the responsibility of domestic authorities

[Former Rec 1] Parties should fully implement and apply the provisions of the Budapest Convention on Cybercrime, including preservation powers (follow up to T-CY Assessment Report 2012).
[Former Rec 2] Parties should consider maintaining statistics or establish other mechanisms to monitor the efficiency of the mutual legal assistance process related to cybercrime and electronic evidence.
[Former Rec 3] Parties should consider allocating more and more technology-literate staff for mutual legal assistance not only at central levels but also at the level of institutions responsible for executing requests (such as local prosecution offices).
[Former Rec 4] Parties should consider providing for better training to enhance mutual legal assistance, police-to-police and other forms of international cooperation on cybercrime and electronic evidence. Training and experience exchange should in particular target prosecutors and judges and encourage direct cooperation between judicial authorities. Such training should be supported by the capacity building programmes of the Council of Europe and other organisations.
[Former Rec 9] Parties and the Council of Europe should work toward strengthening the role of 24/7 points of contact in line with Article 35 Budapest Convention, including through: a. Ensuring, pursuant to article 35.3 Budapest Convention that trained and equipped personnel is available to facilitate the operative work and conduct or support mutual legal assistance (MLA) activities b. Encouraging contact points to pro-actively promote their role among domestic and foreign counterpart authorities; c. Conducting regular meetings and training of the 24/7 network among the Parties; d. Encouraging competent authorities and 24/7 points of contact to consider procedures to

[24] [The previous numbering of recommendations is provided here for ease of reference]

follow up to, monitor the processing and provide feedback to the requesting State on Article 31 requests; e. Considering to establish, where feasible, contact points in prosecution offices to permit a more direct role in mutual legal assistance and a quicker response to requests; f. Facilitating 24/7 points of contact to play a supportive role in "Article 31" requests.
[Former Rec 10] Parties should consider streamlining the procedures and reduce the number of steps required for mutual assistance requests at the domestic level. Parties should share good practices in this respect with the T-CY.
[Former Rec 13] Parties should make use of all available channels, not just formal mutual legal assistance, for international cooperation.
[Former Rec 15] Parties are encouraged to establish emergency procedures for requests related to risks of life and similar exigent circumstances. The T-CY should document practices by Parties and providers.
[Former Rec 16] Parties should confirm receipt of requests systematically and give notice of action taken.
[Former Rec 18] Parties should consider the opening of domestic investigation upon a foreign request or spontaneous information to facilitate the sharing of information or accelerate MLA.
[Former Rec 20] Parties should make use of electronic transmission of requests in line with Article 25.3 Budapest Convention.
[Former Rec 21] Parties should ensure that requests are specific and complete with all necessary information.
[Former Rec 22] Pursuant to Article 25.5 Budapest Convention and Paragraph 259 Explanatory Report, Parties are reminded to apply the dual criminality standard in a flexible manner that will facilitate the granting of assistance.
[Former Rec 23] Parties are encouraged to consult with authorities of requested Party prior to sending requests, when necessary.
[Former Rec 24] Parties should consider ensuring transparency regarding requirements for mutual assistance requests, and reasons for refusal, including thresholds for minor cases, on the websites of central authorities.

5.2.2 Recommendations falling primarily under the responsibility of the T-CY

[Former Rec 8] The T-CY should facilitate greater harmonisation and transparency regarding the time period for data preservation upon a foreign preservation request in line with Article 29 Budapest Convention. The T-CY should document time periods.

5.2.3 Recommendations falling primarily under the responsibility of Council of Europe capacity building projects

[Former Rec 19] The Council of Europe should – under capacity building projects – develop standardised, multi-language templates for Article 31-requests.
[Former Rec 26] The Council of Europe should explore the possibility of establishing an online resource providing information on laws of Parties on electronic evidence and cybercrime as well as on legal thresholds, and evidentiary and other requirements to be met to obtain the disclosure of stored computer data for use in court proceedings.

5.2.4 Recommendations that may need to be addressed through an Additional Protocol to the Budapest Convention on Cybercrime

[Former Rec 6] Parties should consider allowing – via legal domestic amendments and international agreement – for the expedited disclosure of the identity and physical address of the subscriber of a specific IP address or user account.
[Former Rec 7] Parties should consider the possibility and scope of an international production order to be directly sent by the authorities of a Party to the law enforcement authorities of another Party without a formal MLA request.
[Former Rec 12] Parties should consider enhancing direct cooperation between judicial authorities in mutual legal assistance requests.
[Former Rec 14] Parties are encouraged to enable law enforcement and prosecution services to obtain specified traffic and subscriber data directly from foreign service providers, subject to safeguards and conditions.
[Former Rec 17] Parties should consider joint investigations and/or the establishment of joint investigation teams between Parties.
[Former Rec 25] Parties should consider allowing for requests to be sent in English language. Parties should in particular allowing for preservation requests to be sent in English.

Note: Some of these recommendations could partly be addressed also at the domestic level although addressing them through a Protocol may facilitate their acceptance by the international community.

5.3 Follow up

Parties are invited to follow up on recommendations falling under the responsibility of domestic authorities to report back to the T-CY no later than 18 months from adoption of this report on measures taken to permit the T-CY, in line with the Rules of Procedure (Article 2.1.g), to review progress made.

The Council of Europe Secretariat is requested to follow up on recommendations falling under its responsibility and to report back to the T-CY within 18 months of adoption of the report.

The T-CY is to assess the feasibility of taking up recommendations representing "protocol material" in an Additional Protocol to the Convention on Cybercrime.

6 Appendices

6.1 Listing of solutions proposed to make mutual assistance more efficient

Responding States proposed a large number of solutions to make mutual legal assistance more efficient. These are summarised here without judgement as to their feasibility or acceptability by the Parties to the Convention on Cybercrime. Most of these solutions are reflected in the "recommendations" of the present report.

Proposal 1: Fully implement the Convention on Cybercrime

1a Fully implementing the Convention on Cybercrime, including by preserving stored data.

1b Fully implementing the Cybercrime Convention in the law of State Parties.

Proposal 2: Resources – More staff for mutual legal assistance

2a More staff dedicated to cyber issues in local prosecutors' offices (if they are executing requests following reception).

2b More technologically-literate staff for central authorities, because evidence will only become more international, not less.

Proposal 3: Better training

3a Parties: Encouraging States to enhance mutual assistance, via best practices and activities (conferences, workshops and other) and allocation of resources. Council of Europe (through capacity building programmes) and T-CY to support such activities.

3b Central/competent authorities for MLA: Capacity building for central/competent authorities, including training, sharing of experience and good practices on mutual assistance on cybercrime and e-evidence, improvement of procedures, expeditious handling of MLA requests and other activities.

3c Judicial authorities: Sharing of good practices, training and improved procedures to encourage direct communication between judicial authorities.

3d Judges and prosecutors: More comprehensive training and involvement of judges and prosecutors in matters related to cybercrime and electronic evidence, including the use of the Budapest Convention.

3e Law enforcement authorities: Enhance cooperation between law enforcement agencies (LEAs) through seminars, questionnaires, establishment of national Centres of excellence at the national and regional levels (for example through Council of Europe capacity building projects).

Proposal 4: Better knowledge of the requirements of other States

4a Setting up an online resource providing up-to-date information on legal thresholds, evidentiary requirements, guidelines for obtaining data, and other requirements to be met by MLA requests for the disclosure of stored data for use in court proceedings.

4b Establishing a database of laws of Parties on electronic evidence and related criminal offences.

4c Maintaining up-to-date contact lists.

Proposal 5: Changes to the powers of the police

5a Allowing, via legal amendments, for the faster and direct obtaining of subscriber information by a police body, without requiring a court order.

5b Harmonising national legislations, allowing police and judicial authorities to obtain basic identification data without letters rogatory.

5c Empowering the 24/7 points of contact to partially disclose stored data, except content data.

5d Enhancing the powers of the police in obtaining traffic data (subject to co-validation mechanisms by the judicial authorities).

(Note: T-CY comments suggest that these are complex proposals that require further discussion. The disclosure of traffic data may require a court decision. Harmonisation among all the Parties may be difficult to achieve.)

Proposal 6: Changes to legal regimes

6a Developing a faster and simplified MLA regime among Parties to the Cybercrime Convention.

6b Reviewing the legal concept of traffic data and subscriber information. This may require adjustments to the EU Data Retention Directive with respect to the type of data covered.

6c Identifying solutions to facilitate the expeditious obtaining and disclosure of subscriber information to foreign authorities, possibly without or with a "light" MLA procedure (such as formal validation if the data is used in criminal proceedings). Procedures, criteria and safeguards to be agreed upon.

6d Enabling law enforcement authorities to apply for warrants to access stored communications following a mutual assistance request from a foreign country.

6e Establishing, in accordance with legislators and Internet Service Providers (ISPs), a protocol allowing for the disclosure of certain types of data without judicial request or letter rogatory.

6f Enabling law enforcement to obtain stored traffic data from an ISP and pass that data on to a foreign LEA without a formal mutual assistance request (Note: Comments underline that in some countries disclosure of traffic data requires a court decision).

6g Allowing 24/7 contact points to handle directly MLA requests.

6h Preparing an international agreement regarding jurisdiction if the headquarters of a company is in one country, but the servers in another, or even several countries in order to better identify the target of a request for data (Note: Comments suggest such jurisdictional rules are considered a complex question and difficult to negotiate).

Proposal 7: Make use of preservation powers

7a Fully implementing the Convention on Cybercrime, including the specific preservation powers of Articles 16, 17, 29 and 30.[25]

7b Enabling the police to require stored communications held by an ISP to be preserved on behalf of a foreign law enforcement authority pending the receipt of a formal mutual assistance request.

7c Making greater use of preservation powers so as to speed up the process and ensuring that data is not destroyed.

7d Ensuring both the preservation and retention of the data.

Proposal 8: Time periods for storage of data by Internet service providers

8a Time-limits of data storage prescribed by law (preservation and retention) should be made more transparent.

8b Further regulating and harmonising the time limits set for the storage of data.

8c Harmonising time periods for data preservation among States.

Proposal 9: Role of 24/7 points of contact in mutual legal assistance requests

9a 24/7 points of contact should become more pro-active and make themselves known to relevant criminal justice authorities within their country, as well as to foreign competent authorities.

9b Organising common meetings and trainings of the 24/7 network, to enhance its efficiency.

9c 24/7 points of contact should play at least a supportive role in "Article 31" requests, in line with Article 35 Budapest Convention.

9d 24/7 points of contact may be established within the office of the prosecutor to allow for a wider range of actions and a quicker response to requests. Transferring, if necessary, 24/7 contact points from LEA to the prosecution, while establishing LEA as secondary contact points.

9e Competent authorities and 24/7 points of contact should consider procedures to follow up to, monitor the processing and provide feedback to the requesting State on Article 31 requests.

9f Countries may consider mechanisms to allow 24/7 contact points to handle directly MLA requests, including their execution.

9g Enabling 24/7 contact points to directly send or receive requests (without the intervention of the Ministry of Justice with obligatory notification of the relevant Ministry of Justice or prosecutor.

9h Establish procedures and pro-active cooperation between 24/7 contact points and competent authorities for MLA at the level of prosecution services and Ministries of Justice. Establishing contact points at the level of the central authority (Ministry of Justice), the prosecution and the police.

9i 24/7 points of contact: Organising common meetings and trainings of the 24/7 network, to enhance its efficiency.

9j 24/7 points of contact: Ensuring, pursuant to article 35.3 Budapest Convention that trained and equipped personnel is available to facilitate the operative work and conduct or support mutual legal assistance (MLA) activities.

---

[25] See T-CY Assessment Report on preservation: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/TCY_2012_10_Assess_report_v30_public.pdf

Proposal 10: Direct communication between cybercrime units or 24/7 contact points

10a Enhance direct communication between cybercrime units and 24/7 contact points of the Parties.

Proposal 11: Direct communication between prosecutors' offices

11a 24/7 points of contact may be established within the office of the prosecutor to allow for a wider range of actions and a quicker response to requests.

Proposal 12: Direct communication between central authorities and/or judicial authorities

12a Establishing contact points at the level of the central authority (Ministry of Justice), the prosecution and the police for Article 31 and similar requests.

12b States should make use of the possibilities for direct cooperation between judicial authorities, in particular since requests related to cybercrime and electronic evidence are usually considered as urgent. Article 4 of the 2nd Additional Protocol to the Convention on Mutual Legal Assistance in Criminal Matters and other regional and bi-lateral agreements allow for direct cooperation. This would reduce the pressure on central authorities.

Proposal 13: Alternative channels of communication

13a Possible coordination between the Budapest Convention's 24/7 points of contact and the partially overlapping Interpol points of contact.

13b Use of all available international channels of cooperation, including Eurojust and the European Judicial Network.

13c INTERPOL channels could be used to ensure swift transmission of urgent MLA requests.

Proposal 14: Requesting non-content data directly from multi-national Internet service providers

14a Enabling authorized law enforcement and prosecution to directly request traffic and subscriber data from ISPs. Criteria, safeguards and conditions to be determined. These may include domestic court orders.

14b Engaging in direct contact with local representatives of multi-national service providers.

14c Determine the appropriate format and requirements for submission of requests directly to the ISPs. In many cases the requirements are available on the website of the ISP in question.

14d Use of direct contact with foreign ISPs in urgent cases, when tolerated/favoured by the host country (in particular the USA).

14e Engage with ISPs within the context of their existing law enforcement policies that often allow for such direct cooperation with foreign authorities, in particular if they have a legal representation in the requesting State.

Proposal 15: Emergency procedures

15a Emergency procedures should be put in place for requests related to risks of life and similar exigent circumstances.

Proposal 16: Joint investigation teams

16a Joint investigations teams should be set up to deal with complex cases.
16b Establishing joint investigation teams between countries.

Proposal 17: A common template for mutual legal assistance requests

17a Standardised, multi-language templates for "Article 31" requests. This should reduce cost and delays related to translation and ensure that requests are complete and recognised by the other Party.

Proposal 18: Methods for sending mutual assistance requests

18a A tiered/prioritisation system whereby requests must be labelled according to their urgency/importance to ensure that the most urgent requests are prioritised.
18b Making greater use of electronic transmission so as to speed up the process. Favouring email, fax, etc. as means and methods of communication to transmit requests — while also sending in parallel its original version.
18c Considering the development of an electronic secured channel of communication for MLA requests between the Parties.

Proposal 19: Mutual legal assistance procedures in general

19a Preparing standard operating procedures for MLA requests.
19b Prior consultation between central authorities before the formal sending of mutual assistance requests.
19c Using videoconference systems in the context of foreign judicial requests.
19d Encouraging States to enhance mutual assistance and to find solutions for difficult cases.

Proposal 20: The character of requests

20a Ensuring transparency by Parties regarding thresholds for executing MLA requests. The petty character of an offence should not be a ground for denial of mutual assistance request. On the other hand, the MLA system should not be clogged with minor cases. Parties should establish arrangements for the handling of minor cases.
20b Formulating requests as specific and narrow as possible. Overly broad or vague requests are likely to be rejected
20c Having recourse to mutual assistance only in specific cases (facts are related to organised crime. the prejudice reaches a minimum threshold. facts are of an exceptional gravity).
20d Providing as much information as possible in requests. Attachment of necessary documents and/or statements to the request, as well as any other relevant information. At the same time, Parties to find solutions regarding the great amount of information required by the requesting State.

Proposal 21: Languages

21a When translation into the national language of the requested State is not available swiftly, English should be the language favoured in letters rogatory.

21b Favouring English and French languages for correspondence.

21c Using better-qualified translators to ensure higher quality of translated requests. Refraining from using automatic translation programmes.

Proposal 22: Reducing steps and speeding up the process

22a Reducing the number of steps required in the MLA process, including reducing the intermediary organisations.

Proposal 23: Deadlines for responding to mutual legal assistance requests

23a Setting timelines for responding to requests, or giving notice of actions taken.

23b Confirming receipt of requests.

Proposal 24: Other important suggestions

24a Establishing a(n online) forum between stakeholders (MoJ central authority, prosecutors and judges, police, ISPs, banking institutions, financial investigation units, and telecommunication agencies).

24b Request ISPs not to disclose the request to the subject. The policies of most of the ISPs state that they will notify the subject of the access request that a request for access to their information has been received. If the act of notifying the subject of the access request will jeopardise an ongoing criminal investigation, a court order authorising the request for access should also seek to prevent the ISP from notifying the subject of the request.

24c Direct request for stored data from the judicial authority in State A – via 24/7 point of contact – to 24/7 contact point in State B to transmits the request to ISP in State B with copy of the request and results to judicial authorities in State B in order to control that conditions are respected.

6.2 Compilation of relevant domestic legislation[26]

6.2.1 Albania

Law no.1093 date 03.12.2009 "On jurisdictional relations with foreign authorities in criminal matters"

Article 7 of the Forwarding a letter request to the competent authority

1. The Ministry of Justice opens the way to a foreign letter request after it evaluates the conditions defined in the domestic legislation.
Subsequently, the letter request is forwarded to the prosecutor of the district where the letter request is to be executed, through the General Prosecutor.

Article 8 Refusal of the letter request

1. The Ministry of Justice and the local judicial authority open the way to a letter request when the conditions defined in the domestic legislation are met.

Article 16 Presence of foreign judicial authorities in the receipt of evidence

1. At the express request of a foreign judicial authority, the local judicial authority gives information about the time and place of execution of the letter rogatory.
2. The court may permit representatives of foreign judicial authorities to take part in the receipt of evidence and to address questions to the person who is questioned according to the rules of the Code of Criminal Procedure.

Article 22 Searching for and sequestration of objects

1. At the request of foreign judicial authorities, a local judicial authority may order the permission of a search of places or the sequestration of items that can be confiscated which are located in the territory of the Republic of Albania in connection with the facts specified in the letter rogatory. The decision may be appealed within 10 days from the day following receipt of knowledge according to the rules of the Coder of Criminal Procedure.
2. The competent local judicial authority performs the search and sequestration in compliance with the rules of the Code of Criminal Procedure.
3. When a third party, who has gained the right in good faith, a state authority or an injured party who has [his] residence or domicile in Albania claims ownership of the objects, documents or profits, the object provided in point 1 of this article are sent only if the foreign judicial authority guarantees their return at the end of the proceedings in connection with the evidence.
4. The sending may be postponed for as long as the objects, documents or profits are necessary for criminal proceedings that have begun in Albania.

Article 23 Delivery of sequestered objects

1. The objects sequestered are send to the foreign judicial authority at its request, in execution of the letter rogatory, to be confiscated or to be returned to the lawful owner.
2. These objects include:
a) objects used for the commission of a criminal offence;
b) objects that come from the commission of a criminal offence or values equivalent to them;

[26] Based on replies to questionnaire and/or Country Profiles

c) profits from a criminal offence or values equivalent to them;
ç) other objects given with the purpose of inciting the commission of a criminal offence as well as compensation for a criminal offence.
3. The objects or profits may be kept in a permanent manner in Albania if:
a) their owner has [his] residence or domicile in the Republic of Albania;
b) there are serious claims of the Albanian state authorities in connection with the objects or profits;
c) a person, who has not taken part in the commission of a criminal offence and whose claims are not guaranteed by the requesting state proves that he has earned the right to those objects and profits in good faith, as well as that the person has [his] residence in Albania.

Article 24 Postponing the execution of requests

1. A local judicial authority may postpone or condition the execution of requests if it may affect the good conduct of criminal proceedings started by local judicial authorities.
2. The local judicial authority notifies the foreign judicial authority, declaring the reasons for postponement or conditioning. If the notification is made directly to the foreign judicial authority, the local judicial authority informs the Ministry of Justice at the same time.

Article 27 of Law on "On the Jurisdictional Relations with Foreign Authorities in Criminal Matters"

Forwarding data without a request
1. Local judicial authorities even on their own initiative forward to foreign judicial authorities information that is related to criminal offences collected during a criminal proceeding, if they judge that forwarding such information may assist in the opening of a criminal proceeding or the submission of a request for legal assistance from the foreign state. This information is forwarded if the progress of the criminal proceeding in Albania is not hindered and respecting the conditions of reciprocity.
2. The competent local judicial authority may ask the foreign judicial authorities that have received the information mentioned in the first point of this article for data about the measures taken in connection with the information forwarded. In addition, the competent local judicial authority may establish other conditions related to the use of this information in the state to which the information has been forwarded.

Criminal Procedure Code

Article 505 The competencies of the Minister of Justice

1. The Minister of Justice decides to grant support to a letter of application of a foreign authority regarding communications, notifications and the taking of proofs, except when evaluates that the requested actions impair the sovereignty, the security and important interests of the state.
2. The Minister does not grant support to the letter of application when it is certain that the requested actions are prohibited expressly by law or contradict the fundamental principles of the Albanian rule of law. The Minister does not grant support to the letter of application when there are motivated reasons to think that the considerations regarding race, religion, sex, nationality, language, political beliefs or the social state may cause a negative influence to the performance of the process, and when it is certain that the defendant has expressed freely his consent for the letter of application.
3. In cases the letter of application has as subject the summons of the witness, expert or a defendant before a foreign judicial authority, the Minister of Justice does not grant support to the letter of application when the requesting state does not give sufficient guarantee for the non-encroachment of the cited person.
4. The Minister has the right to not grant support to the letter of application in case the requesting state does not give the necessary guarantee of reciprocity.

Article 506 The court proceedings

1. The foreign letter of application cannot be executed unless the court of the place where he must be proceeded has rendered a favourable decision rendered.
2. The district prosecutor, after taking the acts from the Minister of Justice, submits his request to the court.
3. The court disposes of the execution of the letter of application by a decision.
4. The execution of the letter of applications not accepted:
a) in cases the Minister of Justice does not grant support to the letter of application
b) when the fact for which the foreign authority proceeds is not provided as a criminal offence by the Albanian law.

6.2.2 Australia

Mutual Assistance in Criminal Matters Act 1987

Sec. 8 of Mutual Assistance in Criminal Matters Act 1987 of Australia Refusal of assistance

(1) A request by a foreign country for assistance under this Act shall be refused if, in the opinion of the Attorney-General:
(a) the request relates to the prosecution or punishment of a person for an offence that is, or is by reason of the circumstances in which it is alleged to have been committed or was committed, a political offence; or
(b) there are substantial grounds for believing that the request has been made with a view to prosecuting or punishing a person for a political offence; or
(c) there are substantial grounds for believing that the request was made for the purpose of prosecuting, punishing or otherwise causing prejudice to a person on account of the person's race, sex, religion, nationality or political opinions; or
(d) the request relates to the prosecution or punishment of a person in respect of an act or omission that if it had occurred in Australia, would have constituted an offence under the military law of Australia but not also under the ordinary criminal law of Australia; or
(e) the granting of the request would prejudice the sovereignty, security or national interest of Australia or the essential interests of a State or Territory; or
(f) the request relates to the prosecution of a person for an offence in a case where the person has been acquitted or pardoned by a competent tribunal or authority in the foreign country, or has undergone the punishment provided by the law of that country, in respect of that offence or of another offence constituted by the same act or omission as that offence.
(1A) A request by a foreign country for assistance under this Act must be refused if it relates to the prosecution or punishment of a person charged with, or convicted of, an offence in respect of which the death penalty may be imposed in the foreign country, unless the Attorney-General is of the opinion, having regard to the special circumstances of the case, that the assistance requested should be granted.
(1B) A request by a foreign country for assistance under this Act may be refused if the Attorney-General:
(a) believes that the provision of the assistance may result in the death penalty being imposed on a person; and
(b) after taking into consideration the interests of international criminal co-operation, is of the opinion that in the circumstances of the case the request should not be granted.

(2) A request by a foreign country for assistance under this Act may be refused if, in the opinion of the Attorney-General:
(a) the request relates to the prosecution or punishment of a person in respect of an act or omission that, if it had occurred in Australia, would not have constituted an offence against Australian law; or
(b) the request relates to the prosecution or punishment of a person in respect of an act or omission that occurred, or is alleged to have occurred, outside the foreign country and a similar act or omission occurring outside Australia in similar circumstances would not have constituted an offence against Australian law; or
(c) the request relates to the prosecution or punishment of a person in respect of an act or omission where, if it had occurred in Australia at the same time and had constituted an offence against Australian law, the person responsible could no longer be prosecuted by reason of lapse of time or any other reason; or
(d) the provision of the assistance could prejudice an investigation or proceeding in relation to a criminal matter in Australia; or
(e) the provision of the assistance would, or would be likely to, prejudice the safety of any person (whether in or outside Australia); or
(f) the provision of the assistance would impose an excessive burden on the resources of the Commonwealth or of a State or Territory; or
(g) it is appropriate, in all the circumstances of the case, that the assistance requested should not be granted.

Sec.10- Request by Australia

(1) A request for international assistance in a criminal matter that Australia is authorised to make under this Act may be made only by the Attorney-General.

(2) Subsection (1) does not prevent the Attorney-General on behalf of Australia from requesting international assistance in a criminal matter other than assistance of a kind that may be requested under this Act.

Sec.11- Request by foreign country

(1) A request by a foreign country for international assistance in a criminal matter may be made to the Attorney-General or a person authorised by the Attorney-General, in writing, to receive requests by foreign countries under this Act.
(2) A request must be in writing and must include or be accompanied by the following information:
(a) the name of the authority concerned with the criminal matter to which the request relates;
(b) a description of the nature of the criminal matter and a statement setting out a summary of the relevant facts and laws;
(c) a description of the purpose of the request and of the nature of the assistance being sought;
(d) any information that may assist in giving effect to the request.
However, a failure to comply with this subsection is not a ground for refusing the request.
(3) Where a request by a foreign country is made to a person authorised under subsection (1), the request shall be taken, for the purposes of this Act, to have been made to the Attorney-General.
(4) If a foreign country makes a request to a court in Australia for international assistance in a criminal matter:
(a) the court must refer the request to the Attorney-General; and
(b) the request is then taken, for the purposes of this Act, to have been made to the Attorney-General.

15B Requests by foreign countries for stored communications

The Attorney-General may, in his or her discretion, authorise the Australian Federal Police or a police force or police service of a State, in writing, to apply for a stored communications warrant under section 110 of the Telecommunications (Interception and Access) Act 1979 if the Attorney-General is satisfied that:

(a) an investigation, or investigative proceeding, relating to a criminal matter involving an offence against the law of a foreign country (the **requesting country**) has commenced in the requesting country; and
(b) the offence to which the investigation, or investigative proceeding, relates is punishable by a maximum penalty of:
(i) imprisonment for 3 years or more, imprisonment for life or the death penalty; or
(ii) a fine of an amount that is at least equivalent to 900 penalty units; and
(c) there are reasonable grounds to believe that stored communications relevant to the investigation, or investigative proceeding, are held by a carrier; and
(d) the requesting country has requested the Attorney-General to arrange for access to the stored communications.

Telecommunications (Interception and Access) Act 1979

110 Enforcement agencies may apply for stored communications warrants

(1)An enforcement agency may apply to an issuing authority for a stored communications warrant in respect of a person.
(2)The application must be made on the agency's behalf by:
(a)if the agency is referred to in subsection 39(2)—a person referred to in that subsection in relation to that agency; or
(b)otherwise:
(i)the chief officer of the agency; or
(ii)an officer of the agency (by whatever name called) who holds, or is acting in, an office or position in the agency nominated under subsection (3).
(3)The chief officer of the agency may, in writing, nominate for the purposes of subparagraph (2)(b)(ii) an office or position in the agency that is involved in the management of the agency.
(4)A nomination under subsection (3) is not a legislative instrument.

116 Issuing of stored communications warrants

(1)An issuing authority to whom an enforcement agency has applied for a stored communications warrant in respect of a person may, in his or her discretion, issue such a warrant if satisfied, on the basis of the information given to him or her under this Part in connection with the application, that:
(a)Division 1 has been complied with in relation to the application; and
(b)in the case of a telephone application—because of urgent circumstances, it was necessary to make the application by telephone; and
(c)there are reasonable grounds for suspecting that a particular carrier holds stored communications:
(i)that the person has made; or
(ii)that another person has made and for which the person is the intended recipient; and
(d)information that would be likely to be obtained by accessing those stored communications under a stored communications warrant would be likely to assist in connection with:
(i)in the case of an application other than a mutual assistance application—the investigation by the agency of a serious contravention in which the person is involved (including as a victim of the serious contravention); or
(ii)in the case of a mutual assistance application—the investigation or investigative proceeding, by the foreign country to which the application relates, of a serious foreign contravention to which the application relates and in which the person is involved (including as a victim of the serious foreign contravention); and
(da)if the stored communications warrant is applied for in relation to a person who is the victim of the serious contravention—the person is unable to consent, or it is impracticable for the person to consent, to those stored communications being accessed; and
(e)in any case—having regard to the matters referred to in subsection (2) or (2A) (as the case requires), and to no other matters, the issuing authority should issue a warrant authorising access to such stored communications.

117 What stored communications warrants authorise

A stored communications warrant authorises persons approved under subsection 127(2) in respect of the warrant to access, subject to any conditions or restrictions that are specified in the warrant, a stored communication:
(a)that was made by the person in respect of whom the warrant was issued; or
(b)that another person has made and for which the intended recipient is the person in respect of whom the warrant was issued;
and that becomes, or became, a stored communication before the warrant is first executed in relation to the carrier that holds the communication.

6.2.3 Austria

Article 3 paragraph 2 of the Statute for Police cooperation enables safety authorities in to accomplish mutual assistance

The law enforcement authorities are obliged to render legal assistance also without being requested,

1. by using data that have – owing to their nature – to be transmitted under international law, or
2. if required by a foreign law enforcement authority for the purpose of fulfilling its duties pursuant to s.1, p.1, which states that the International cooperation serves the purposes of the law enforcement (police), CID (Criminal Investigation Division), passport authorities, Aliens Police, and border control on condition of reciprocity,
3. if required for criminal investigation activities by Interpol.

Section 56 para 2 of the Austrian Federal Law on Extradition and Mutual Legal Assistance reads as follows:

"A request for a search of persons or premises, the seizure of objects or monitoring of telecommunications must have attached the original or a certified copy or photocopy of the order from the relevant authority. If not a court order, there must be a statement from the authority seeking the mutual assistance that the conditions required for such measures under applicable law in the requesting country are satisfied."

Extradition and Mutual Assistance Act (ARHG)

Section 3. Reciprocity

(1) A foreign request shall only be complied with provided that it is guaranteed that the requesting State would also comply with a similar request by Austria.

(2) A request may not be filed under this law by an Austrian authority if a similar request by another State were not able to be complied with, except in the event that a request appears to be needed urgently for specific reasons. In this case the requested State shall be notified of the lack of reciprocity.

(3) In the event of doubt over observance of reciprocity, the opinion of the Federal Minister of Justice shall be sought.

(4) Another State may be guaranteed reciprocity in connection with a request made under this law, provided that no intergovernmental agreement exists and that it would be permissible under this law to comply with a similar request of this State.

Direct applicability of the Convention upon its ratification by Austria; see also Section 58 ARHG in connection with Section 143 seq. of the Austrian Code of Criminal Procedure respectively Section 115 of the revised Code of Criminal Procedure (in force from 2008-1-1)

Section 55. Jurisdiction for Processing Letters Rogatory

(1) The district court is competent to process letters rogatory, sections 2 and 3 notwithstanding; in cases where under the 1975 Code of Criminal Procedure, the decision is reserved for the *Ratskammer* or in which there is a request for a search, seizure, temporary injunction or a decision under section 145a of the Code of Criminal Procedure, the court of justice of the first instance in whose district the mutual assistance procedure is to be brought has jurisdiction. Sections 23 and 24 of the 1988 Youth Court Act are applicable as appropriate. If approval of cross-border observation is sought, the court of justice of the first instance in whose district the border will probably be crossed has jurisdiction; in case of observation in an aircraft that flies into Austria,

however, the court of justice in whose district the landing site is located has jurisdiction. Information about a criminal procedure, execution of a prison sentence or preventive measures is issued by the court with jurisdiction; for requests for the transfer of records, the office in which the records are kept has jurisdiction. If a person detained in the prison of a court of justice is to be interrogated, that court of justice has jurisdiction. If the jurisdiction cannot be determined according to these rules, the District Court of the Inner City of Vienna, in cases in which the decision is reserved for the court of justice of the first instance, the Regional Criminal Court of Vienna has jurisdiction.

(2) If a person to be transferred is in prison or preventive custody, the decision on the request for transfer is made by a single judge of the court given in section 16 of the Penal Sentence Enforcement Act, otherwise it is the court on whose order the detention is based. The Federal Ministry of Justice is to be informed of this decision. The Federal Minister of Justice must refuse the transfer if one of the circumstances listed in sections 2 and 3 (1) is present. Transfer at the appropriate border crossing or any other transfer site agreed to be performed by police officers of the Ministry of Justice.

(3) If a person detained in another state is to be transferred through Austria to a third state for important investigative activities, in particular their interrogation or confrontation, sections 44, 47 and 49 apply as appropriate

Direct applicability of the Convention upon its ratification by Austria; to be noted that under Section 3 of the ARHG, mutual assistance can be granted in the absence of a treaty on the basis of reciprocity

Section 58. Applicable Procedures

Mutual assistance is to be provided according to the provisions for criminal procedures within Austria. A request to follow a specific deviating procedure will be granted if this procedure is consistent with the principles of Austrian criminal procedure. If mutual assistance is provided in the form of confiscation (section 143 of the 1975 Code of Criminal Procedure) or a temporary injunction (section 144a of the 1975 Code of Criminal Procedure), this is to be limited in time; the foreign authority making the request is to be informed in the appropriate way.

Section 65

(1) For other criminal offences committed abroad than those referred to in sections 63 and 64 applies the Austrian criminal law, if the offences are also liable to persecution according to the laws which are valid for the scene of the crime:

1. if the offender has been Austrian at the time of the offence or if he has acquired Austrian citizenship at a later date and if he still holds citizenship at the time of initiation of the criminal proceedings;

6.2.4 Bosnia and Herzegovina

Law on Mutual Legal Assistance in Criminal Matters (The Official Gazette of Bosnia and Herzegovina, no. 53/09, 58/13)

Article 3 Letter Rogatory

(1) Request for mutual legal assistance shall be transmitted in the form of Letter Rogatory.
(2) The Letter Rogatory of a foreign judicial authority and the attached documentation must be supported by the translation into one of the official languages of Bosnia and Herzegovina. The translation must be verified by a certified court interpreter.
(3) The Letter Rogatory by a national judicial authority and the attached documentation must be translated into the official language of the requested State.

Article 4 Channels of Communication

(1) Letters Rogatory requesting mutual legal assistance of the national judicial authorities shall be transmitted to foreign judicial authorities through the Ministry of Justice of Bosnia and Herzegovina. Requests for mutual assistance of foreign judicial authorities shall be transmitted to the national judicial authorities through the same channel.
(2) As an exception to Paragraph (1) of this Article, national judicial authorities may directly address the request for mutual legal assistance to a foreign judicial authority, when such a communication is envisaged by an international treaty.
(3) In urgent cases, when such a communication is envisaged by an international treaty, requests for mutual legal assistance may be transmitted and received through the Interpol.
(4) In urgent cases, letters rogatory may be sent and received through Eurojust.
(5) Procedure of competent bodies of Bosnia and Herzegovina in relations with Eurojust, shall be regulated by specific instruction of Miniser of Justice of Bosnia and Herzegovina, by which institutions and contact point for cooperation with Europol will be appointed.
(6) In cases of communication referred to in Paragraphs (2) and (3) of this Article, the national judicial authority shall communicate a copy of the request for mutual legal assistance to the Ministry of Justice of Bosnia and Herzegovina.
(7) The Ministry of Justice of Bosnia and Herzegovina shall transmit and receive through the Ministry of Foreign Affairs of Bosnia and Herzegovina the requests for mutual legal assistance to/from a foreign State that has no international treaty in force with Bosnia and Herzegovina, as well as in cases when an international treaty explicitly envisages use of diplomatic channels of communication.
(8) Requests for mutual legal assistance may also be received if transmitted via electronic or some other means of telecommunication with a written record, and if the foreign relevant judicial authority is willing, upon request, to deliver a written evidence of the manner of transmission and the original request, provided that this manner of transmission is regulated in an international treaty.
Upon receipt of a request from a foreign 24/7 contact point, which contains all the necessary data, the same is delivered to competent BiH police bodies for further proceedings.

Article 5 Urgency of Proceeding

(1) The Ministry of Justice of Bosnia and Herzegovina shall transmit, without delay, request for mutual assistance by a foreign judicial authority to the relevant nationaljudicial authority for further action, unless it is evident that the request is not in compliance with an international treaty and this Law, in which case it should be refused.
"(2) The Ministry of Justice of Bosnia and Herzegovina shall urgently act on the request of national judicial authorities, unless it is obvious that the request does not comply with international treaty and it will be refused by foreign authority. In this case, such a request is returned to the national judicial authority to remedy deficiencies. "

(3) In cases referred to in Article 4 Paragraph (3) of this Law, competent body of Bosnia and Herzegovina for cooperation with Interpol shall communicate the request directly to the relevant national judicial authority, therewith a copy of the request and the sending letter shall submit to the Ministry of Justice of Bosnia and Herzegovina

Article 6 Admissibility and Course of Action

(1) The relevant national judicial authority shall decide on the admissibility and course of action in providing mutual legal assistance requested by a foreign judicial authority in compliance with nationalregulations, unless otherwise stipulated by this Law or an international treaty.
(2) The relevant national judicial authority shall proceed on request by the foreign judicial authority without delay.

Article 7 Forwarding the Letter Rogatory to Relevant Authority

If the authority to which the Letter Rogatory was transmitted is not authorized to proceed, that authority shall forward it without delay to the relevant authority for action, and shall accordingly inform the authority that transmitted the request.

Article 9 Grounds for refusing of legal assistance

(1) Among other reasons prescribed by this law for refusing requests for certain forms of legal assistance, the relevant national judicial authority shall refuse the request for mutual legalassistance:
a) if the execution of the request would prejudice the legal order of Bosnia and Herzegovina or its sovereignty or security;
b) if the request concerns an offense which is considered to be a political offense or an offense connected with a political offense;
c) if the request concerns a military criminal offense.
d) if the person accused of the relevant criminal offense has been acquitted of charges based on the substantive-legal grounds or if the proceeding against him has been discontinued, or if he was relieved of punishment, or if the sanction has been executed or may not be executed under the law of the country where the verdict has been passed;
e) if criminal proceedings are pending against the person in Bosnia and Herzegovina for the same criminal offense, unless the execution of the request might lead to a decision releasing the accused from custody,
f) if criminal prosecution or execution of a sanction pursuant to the national law would be barred by the statute of limitations
(2) The provisions referred to in Paragraph (1) Sub-paragraph d) of this Article shall not apply in cases of reopening the criminal proceedings in the requesting State.
(3) In addition to the reasons stated in paragraph (1) of this Article, legal assistance may be refused on the basis of factual reciprocity in relation to a particular country.

Article 10 Exceptions for refusing of legal assistance

(1) Crimes against humanity or other values protected by international law may not serve as a basis to deny the request for mutual legal assistance in terms of Article 9 Sub-paragraphs b) and c) of this Law.
(2) No request for mutual legal assistance shall be denied solely because it concerns an offense which is considered to be a fiscal offense pursuant to national law.

Article 11 Reasoning the Failure to Execute the Request

The decision refusing the request to afford mutual legal assistance or the failure to execute the request must be reasoned.

Grounds for refusal to cooperate could be an insufficiently elaborated request. Apart from cases referred to in the Convention, the grounds for refusal to cooperate is found in the inability to proceed in cases where there is no criminal offence.

The request, in accordance with the Law on Mutual legal assistance in Criminal Matters (Art. 3, paragraph 2) must be translated into one of the official languages in use in BiH and certified by an authorized court interpreter.

Article 26 (Providing Information without Request)

(1) Without prejudice to their own investigations or proceedings and subject to reciprocity, national judicial authorities may, without a prior request, forward to the relevant foreign judicial authorities information obtained during their own investigations and related to criminal offences if they consider that the disclosure of such information 12 might assist the receiving State in initiating investigations or criminal proceedings or might lead to a request for mutual assistance by that State.

(2) The relevant national judicial authority shall request from the relevant foreign judicial authority to which it transmitted the information referred to in paragraph (1) of this Article communication on any actions undertaken upon such information and it shall also impose other conditions for the use of such information in the receiving State."

Criminal Procedure Code of Bosnia and Herzegovina[27]

Article 72 a Order to the telecommunications operator

(1) If there are grounds for suspicion that a person has committed a criminal offence, on the basis of motion of the Prosecutor or officials authorized by the Prosecutor, the Court may issue an order to a telecommunications operator or another legal person performing telecommunications services to deliver information concerning the use of telecommunications services by that person, if such information could be used as evidence in the criminal proceedings or in collecting information that could be useful to the criminal proceedings.
(2) In case of emergency, the Prosecutor may order the measures under Paragraph (1) of this Article, in which case the information received shall be sealed until the issuance of the court order. The Prosecutor shall immediately inform the preliminary proceedings judge, who may issue an order within 72 hours. In case the preliminary proceedings judge does not issue the order, the Prosecutor shall return such information unsealed.
(3) Measures under Paragraph (1) of this Article may also be ordered against a person if there are grounds for suspicion that he will deliver to the perpetrator or will receive from the perpetrator information related to the offence, or grounds for suspicion that the perpetrator uses a telecommunication device belonging to this person.
(4) Telecommunications operators or other legal persons who provide telecommunications services shall enable the Prosecutor and police authorities to enforce the measures referred to in Paragraph (1) of this Article."

[27] The same provision has been prescribed by CPC of Republika Srpska, CPC of Federation of Bosnia and Harcegovina and CPC of Brčko District.

6.2.5 Bulgaria

Section III "A" from MINISTRY OF INTERIOR ACT - „Exchange of Information or Data with the Competent Bodies of the European Union Member States for Prevention, Discovery and Investigation of Crimes (new – SG 93/09, in force from 24.11.2009).

Art. 161a. (new – SG 93/09, in force from 24.11.2009)
(1) Following the provisions of this section the MI through a competent specialized structure shall carry out a simplified exchange of information or data with the competent law enforcement administrations of the European Union Member States, and with the states signatories to the Schengen Agreement for prevention, discovery and investigation of crimes.
(2) The Ministry of Interior through a competent specialized structure may provide:
1. Information and data from the Ministry information funds;
2. Information or data, received from other state bodies or local government authorities, from legal entities and natural persons.
(3) Exchange of information or data with the competent bodies of the European Union Member States and of the states signatories to the Schengen Agreement shall be done subject to observance of th, to which the Republic of Bulgaria is a party, and also subject to observance of the provisions of the Protection of Classified Information Act and the Protection of Personal Data Act.

Art. 161c. (new – SG 93/09, in force from 24.11.2009)
(1) Provision of the required information or data may be withdrawn where there are sufficient grounds to reckon that there is danger of:

1. Establishment of conditions threatening national security and public order;
2. Hindering actions of investigation or gathering data for initiation of penal proceedings;
3. Endangering a natural person's safety.

(2) In addition to the cases under par. 1 provision of required information or data may be refused where they:

1. do not correspond to the objectives, for which they have been requested;

2. are related to a crime, for which the law provides a penalty of imprisonment for a period of up to one year or another less grave penalty.
(3) The requested information or data shall be provided only if permission by the competent judicial body for access to them has been obtained.

Conditions
Art. 161e. (new – SG 93/09, in force from 24.11.2009)
(1) Information or data shall be provided on the grounds of a request by the respective competent body of the Member State.
(2) The request for provision of information or data shall be prepared in one of the official languages of the European Union and shall contain:
1. the justifications, that the respective information of data are available;
2. the purpose for which the information or data are requested;
3. the connection between the purpose and the person, to which the information or data relate.
(3) Information or data, required for prevention, discovery or investigation of crimes under Art. 36 of the Extradition and European Arrest Warrant Act, may be provided without addressing a request.

The Electronic communications act –
Article 251Conditions:

- the request should come from competent authority;
- the grounds that the information or data is available in Bulgaria;
- purpose of the requested data;
- what data exactly is needed (subscriber, traffic, etc.);
- period of time for the data (if applicable – traffic data, etc.);
- data is presented to asking party after a court approval (court order issued for the providers)

EXTRADITON AND EUROPEAN ARREST WARRANT ACT

Conditions for application of the European Arrest Warrant

Art. 36. (*) (1) (amend. – SG 49/10) European Arrest Warrant shall be issued for persons who has committed offences, which carry as per the legislation of the requesting country maximum term of not less than one year imprisonment sentence or a measure requiring detention or another more severe penalty, or if the imposed penalty imprisonment or the requiring detention measure is not shorter than 4 months.

(2) The surrender on the base of European Arrest Warrant shall be performed, if the offence which the warrant has been issued for, constitutes a offence as per the Bulgarian legislation too. Execution of an European Arrest Warrant related to taxes, custom fees or currency exchange cannot be refused on the ground that the Bulgarian legislation does not stipulate the same type of taxes or fees or does not settle the taxes, fees, custom fees or the currency exchange in the same way as the legislation of the issuing Member State does.

(3) (Amend. – SG 49/10) Double criminality shall not be required for the following offences, if in the issuing State they carry maximum term of not less than three years of imprisonment or with another more severe penalty, or for them a measure requiring detention for a maximum term of not less than of 3 years is provided:

1. Participation in a criminal organisation,
2. Terrorism,
3. Trafficking in human beings,
4. Sexual exploitation of children and child pornography,
5. Illicit trafficking in narcotic drugs and psychotropic substances,
6. Illicit trafficking in weapons, munitions and explosives,
7. Corruption,
8. fraud, including that affecting the financial interests of the European Communities within the meaning of the Convention of 26 July 1995 on the protection of the European Communities' financial interests,
9. Laundering of the proceeds of offence,
10. Counterfeiting currency, including of the euro,
11. computer-related offence,
12. Environmental offence, including illicit trafficking in endangered animal species and in endangered plant species and varieties,
13. Facilitation of unauthorised entry and residence,
14. murder, grievous bodily injury,
15. illicit trade in human organs and tissue,
16. kidnapping, illegal restraint and hostage-taking,
17. racism and xenophobia,
18. organised or armed robbery,
19. illicit trafficking in cultural goods, including antiques and works of art,
20. swindling,
21. racketeering and extortion,
22. counterfeiting and piracy of products,
23. forgery of administrative documents and trafficking therein,
24. forgery of means of payment,
25. illicit trafficking in hormonal substances and other growth promoters,
26. illicit trafficking in nuclear or radioactive materials,
27. trafficking in stolen vehicles,
28. rape,
29. arson,
30. offences within the jurisdiction of the International Criminal Court,
31. unlawful seizure of aircraft/ships,
32. sabotage

Criminal Procedure Code

Article 471 Grounds and contents of international legal assistance

(1) International legal assistance in criminal matters shall be rendered to another state under the provisions of an international treaty executed to this effect, to which the Republic of Bulgaria is a party, or based on the principle of reciprocity. International legal assistance in criminal cases shall also be made available to international courts whose jurisdiction has been recognised by the Republic of Bulgaria.
(2) International legal assistance shall comprise the following:
1. Service of process;
2. Acts of investigation;
3. Collection of evidence;
4. Provision of information;
5. Other forms of legal assistance, where they have been provided for in an international agreement to which the Republic of Bulgaria is a party or have been imposed on the basis of reciprocity.

6.2.6 Costa Rica

Article 24 of the Political Constitution of the Republic of Costa Rica:
http://www.pgr.go.cr/scij/busqueda/normativa/normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=871&nValor3=88326&strTipM=TC

Law on Registry, Kidnapping and Examination of Private Documents and Intervention of the Communications:
http://www.pgr.go.cr/Scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=16466&nValor3=17615&param2=1&strTipM=TC&lResultado=3&strSim=simp

Public Ministry's Statutory Law and the Penal Procedural Code:
http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=27760&nValor3=29368&param2=1&strTipM=TC&lResultado=1&strSim=simp

http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=41297&nValor3=91419&param2=2&strTipM=TC&lResultado=12&strSim=simp

6.2.7 Croatia

Act on international legal assistance in criminal matters (Official Gazette 178/04):

Article 4

International legal assistance is afforded in the widest sense in accordance with the principles of domestic order public, the principles of the European Convention for the Protection of Human Rights and Fundamental Freedoms and the International Covenant on Civil and Political Rights.

Article 8

(1) The domestic judicial authority shall act further to the request for international legal assistance of a foreign judicial authority if the request was submitted in written form. The request, and the supporting deeds, have to be accompanied by a translation into the Croatian language, and if that is not possible then into the English language. Translations have to be officially certified.
(2) The domestic judicial authority shall act further to the request for international legal assistance of a foreign judicial authority even if the request was submitted electronically or by some other means of telecommunications leaving a written record, if it may establish its authenticity, and if the competent foreign authority is willing, at request, to deliver a written notice about the method of sending the request and the original request.
(3) Unless an international treaty or this Act provide otherwise, the request for international assistance has to include:
1. The place of issuance and the name of the competent foreign authority sending the request.
2. The legal basis for providing international legal assistance.
3. The exact description of the requested international legal assistance and the reason for the request for international legal assistance.
4. The legal name, a short factual and legal description of the criminal offence (unless the request relates to the service of court decisions, submissions, documents, etc.).
5. Accurate data about and citizenship of the person in relation to whom international legal assistance is sought and his position in the procedure.
6. In the case of service of court deeds, the type of deed being forwarded.

Article 12

(1) The competent domestic authority may refuse the request for international legal assistance if:

1. The request concerns an act regarded as a political criminal offence, an act connected with a political criminal offence,
2. The request concerns a fiscal offence,
3. The execution of the request would likely prejudice the sovereignty, security, ordre public or other essential interests of the Republic of Croatia,
4. It can be justifiably presumed that the person whose extradition is sought would be criminally prosecuted or punished in the case of extradition, because of his race, religion, citizenship, affiliation with a specific social group, or because of his political beliefs, or if his position would be aggravated on the grounds of one of the mentioned reasons,
5. The matter involves an insignificant criminal offence.

(2) Criminal offences or attempted criminal offences against values protected by international law and participation in the commission of such criminal offences cannot be the basis for rejecting a request for international legal assistance within the meaning of paragraph 1, item 1 of this Article.
(3) A request for international legal assistance, because of a fiscal offence from paragraph 1, item 2 of this Act shall not be rejected exclusively because it relates to an act which is a fiscal offence under domestic law.

Article 13

(1) The domestic judicial authority shall reject a request for international legal assistance:

1. If the accused person has been declared not guilty of the same criminal offence in the Republic of Croatia, because of material-legal reasons, or if the procedure against him has been discontinued, or if he has been released from his sentence, or if the sanction has been enforced or cannot be enforced according to the law of the state in which the judgment was adopted,
2. If a criminal proceeding for the same criminal offence is pending in the Republic of Croatia against the accused person, unless the enforcement of the request could lead to a decision on the release of the accused person,
3. If criminal prosecution, enforcement of the sanction or of the security or protective measure would be barred by the statute of limitations under national legislation.

(2) The provisions of paragraph 1, items 1 and 3 of this Article are not applicable in cases where the final judgment was revised in the requesting state.

1) the form of the international legal assistance requested and the reason for the letter rogatory;
2) legal qualification of the criminal offence committed and the summary of the facts, except if the letter rogatory refers to the service of court writs (applications, documents and the like);
3) nationality and other personal details of the person regarding which the international legal assistance is requested and his status in the proceedings;
4) in case of service of court writs, their type.

Article 18

(1) By not interfering with their own investigations or procedures, and under the condition of reciprocity, domestic judicial authorities may send without a prior request to the competent foreign judicial authorities information relating to criminal offences or to infringements of the rule of law from Article 1, paragraph 3 of this Act, gathered in their own investigations, if they believe that the delivery of such information could be of help in the initiation or implementation of an investigation or court procedure or if they could lead to the submission of a request for legal assistance.

(2) The domestic judicial authority shall request from the foreign judicial authority to which it delivered the information from paragraph 1 of this Article notifications about any actions taken further to such information, as well as a copy of all decisions, and it may also impose other conditions for the use of such information in the receiving state.

(3) The information from paragraph 1 of this Article is forwarded through the Ministry of Justice.

6.2.8 Estonia

CPC § 436. Prohibition on international co-operation in criminal procedure

(1) The Republic of Estonia refuses to engage in international co-operation if:
1) it may endanger the security, public order or other essential interests of the Republic of Estonia;
2) it is in conflict with the general principles of Estonian law;
3) there is reason to believe that the assistance is requested for the purpose of bringing charges against or punishing a person on account of his or her race, nationality or religious or political beliefs, or if the situation of the person may deteriorate for any of such reasons.

(1^1) The Republic of Estonia shall not refuse to engage in international co-operation with a Member State of the European Union on the ground that the offence is regarded as a political offence, as an offence connected with a political offence or an offence inspired by political motives unless otherwise provided by law or an international agreement.

CPC § 460. Requirements for requests for assistance

(1) A request for assistance shall set out:
1) the name of the authority making the request;
2) the content of the request;
3) the name, address and, if possible, other contact details of the person with regard to whom the request is submitted;
4) the facts relating to and the legal assessment of the criminal offence concerning which the request is submitted.

CPC § 461. Prohibition on compliance with request for assistance

Compliance with a request for assistance is not permitted and shall be refused on the grounds provided for in § 436 of this Code.

CPC § 462. Proceedings conducted by Ministry of Justice and Public Prosecutor's Office concerning requests for assistance received from foreign states

(1) The Ministry of Justice shall verify whether a request for assistance received from a foreign state meets the requirements. A request in compliance with the requirements shall be immediately sent to the Public Prosecutor's Office.
(2) The Public Prosecutor's Office shall verify whether compliance with the request is admissible and possible and forward the request to the competent judicial authority for execution.
(2^1) In cases of urgency, a request submitted through the International Criminal Police Organisation (Interpol) or a notice in the Schengen Information System may complied with the consent of the Public Prosecutor's Office before the request for assistance is received by the Ministry of Justice.
(3) The Ministry of Justice shall forward a request for the service of a summons to the court of first instance of the residence or seat of the person for execution.
(4) If a request for assistance is submitted through Eurojust, Eurojust's National Member for Estonia shall verify whether the request for assistance meets the requirements and whether compliance with the request for assistance is admissible and possible and forward the request to the Estonian competent judicial authority for execution.

CPC § 463. Compliance with requests for assistance received from foreign states

(1) Requests for assistance are complied with pursuant to this Code. At the request of a foreign state, a request may be complied with pursuant to procedural provisions different from the provisions of this Code unless this is contrary to the principles of Estonian law.

(1^1) If summoning of a person to court is required for compliance with a request for assistance, service of the summons shall be organised by the court.
(2) The materials received as a result of compliance with a request shall be sent to the Ministry of Justice through the Public Prosecutor's Office and the Ministry of Justice shall forward the materials to the requesting state.
(3) The materials received as a result of compliance with a request for assistance from a foreign state submitted through Eurojust shall be sent to the requesting state through Eurojust unless otherwise agreed with Eurojust.

6.2.9 Finland

Act on International Legal Assistance in Criminal Matters

Section 8— Language and translations

(1) The request and the accompanying documents shall be in Finnish or in Swedish, or be accompanied by a translation into either of these languages. It may be enacted by Decree that the request and the accompanying documents may be in a foreign language.

(2) A competent authority may execute a request for assistance even where the request and the related documents are in a foreign language provided by Decree or in another foreign language, provided that the execution of the request is not otherwise precluded according to this Act. However, the competent authority may refuse to execute the request, where the request and the documents are not in Finnish or in Swedish, nor accompanied by translations into these languages, if the authority deems that it does not have a sufficient understanding of the language used in the documents. The Ministry of Justice shall be responsible for carrying out translations from foreign languages into Finnish and Swedish as will be enacted by Decree.

(3) A document to be served need not be accompanied by a translation where the service may be executed without a translation under section 17(2).

Section 12— Mandatory grounds for refusal

(1) Assistance shall be refused, where the execution of the request would prejudice the sovereignty, the security or other essential interests of Finland.

(2) Assistance shall be refused, where the execution of the request would be contrary to the principles of human rights and fundamental freedoms or otherwise contrary to Finnish public policy (ordre public).

Section 13— Discretionary grounds for refusal

(1) Assistance may be refused, where:
   (1) the request relates to an offence that is of a political character or an offence under military law only;
   (2) the request relates to an offence, committed by a person who according to Finnish law could no longer be prosecuted by reason of lapse of time, pardon or by any other reason;
   (3) the request relates to an offence which in Finland or in a third State is subject to criminal investigations or under consideration of a prosecution authority or where court proceedings have been initiated;
   (4) the request relates to an offence for which the criminal investigations, prosecution or punishment, or any other punitive sanctions have been waived in Finland or in a third State;
   (5) the request relates to an offence in respect of which the offender has been sentenced or acquitted in Finland or in a third State; or
   (6) the execution of the request would, having regard to the nature of the offence, impose an unreasonable burden on the resources available.

(2) The execution of the request may be postponed, if the execution of the request would cause inconvenience or delay in a criminal investigation, criminal investigations or court proceedings in Finland.

Note:

Regardless of the provisions of general MLA law, assistance will be provided as agreed in international conventions. The Budapest Convention is in force as a law in Finland (similarly as other international conventions to which Finland is a party).

Section 15— Restrictions on coercive measures

(1) Where coercive measures are requested or where the request otherwise involves the use of coercive measures under the Coercive Measures Act (450/1987), such measures shall not be used, where not permitted under Finnish law had the offence to which the request relates been committed in Finland in similar circumstances.

Note: No up to date translation available. However, this legislation states e.g. that paragraph 1 does not apply to preservation order of data referred to in Coercive measures Act.

(2) A suspect or a defendant in criminal proceedings pending in the requesting State who is requested to be examined in Finland in criminal investigations or in court may not be arrested, detained or subjected to a travel ban for the acts or omissions constituting the offence specified in the request.

(3) Where the request relates to the service of a summons to appear before an authority of a foreign State, a Finnish authority may not order the person summoned to obey the summons nor use any measures of compulsion in cases of failure to appear. The duty of witnesses and other persons to obey a summons issued by a court of another Nordic State is governed by the Act on the Duty to Appear Before the Court of Another Nordic Country in Certain Cases (349/1975).

Section 23— Use of coercive measures to obtain evidence or to secure the enforcement of a confiscation order

(1) Search and seizure, telecommunications interception, telecommunications monitoring and technical surveillance in order to obtain evidence as well as identification of persons may be carried out pursuant to a request for assistance made by an authority of a foreign State, if this has been requested or deemed necessary in the execution of the request. (406/1995)

Note: No up to date translation available. However, legislation in force lists also preservation order of data.

(2) Coercive measures may be used upon the request of an authority of a foreign State for the purpose of securing the enforcement in Finland of a confiscation order made or to be made in the requesting foreign State where the order is, or would be, enforceable in Finland.

(3) The use of coercive measures shall be governed by section 15(1) of this Act and by the Coercive Measures Act.

6.2.10 France

Article 695-9-31 à 695-9-47 du Code de procédure Pénale.
http://www.legifrance.gouv.fr/affichCode.do;jsessionid=BD0C632EEFF0AB1BB72863C6DE44A8E9.tpdjo07v_1?idSectionTA=LEGISCTA000024544120&cidTexte=LEGITEXT000006071154&dateTexte=20130411

Art R49-35 à R49-39du Code de procédure pénale
http://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=D9318798D21F74DE01CC2DA1848D15D5.tpdjo03v_2?cidTexte=JORFTEXT000025641035&idArticle=LEGIARTI000025642088&dateTexte=20120407

6.2.11 Georgia

Article 10 of the law "On International Law Enforcement Cooperation" a respective law enforcement agency of Georgia will cooperate with a law enforcement agency of a foreign country in the provision and exchange of the following information:

a) Information and data, which will contribute to the prevention, detection and suppression of crimes;
b) Information and personal data related to wanted persons or persons participating in the commission of crime, or persons suspected to participate therein;
c) Information and data related to the offenders' connections, structures of organized groups; typical methods applied by individual offenders and groups, time, place and **modus operandi** of crimes;
d) Information and data related to the acquisition and registration of firearms by a citizen of Georgia in a foreign country or by a citizen of a foreign country in Georgia;
e) Identification data of a motor vehicle and personal data of its owner or user;
f) Criminal intelligence information;
g) Information on the relevant legislation of Georgia;
h) Other information and data determined by bilateral or multilateral treaty or agreement of Georgia, or by the relevant legislation of Georgia.

in article 2 of the law "On International Cooperation in Criminal Matters" that can be formulated as follows:

1. International cooperation in criminal matters is usually carried out on the basis of international treaty of Georgia;
2. In certain cases international cooperation in criminal matters can be also carried out on the basis of reciprocity and individual agreement in case Georgia does not have relevant international treaty with that foreign state;
3. International cooperation based on the principle of reciprocity can be carried out on all issues enshrined in the 1(1) article of this Law despite the extradition and executing judgement of the court;
4. International cooperation based on the principle of reciprocity can be carried out only if reciprocal conditions are clearly formulated and they contain the minimal guarantees provided by this Law without prejudice to establishing higher standards;
5. Individual agreement (ad hoc agreement) can only be concluded for a certain case of mutual assistance and it should contain the minimal guarantees provided by this Law without prejudice to establishing higher standards.

Article 12 (1) of the law "On Cooperation in Criminal Matters" summarised as follows:

1 Georgia will not execute mutual assistance request in case:

a) Executing a mutual assistance request threatens sovereignty, public security or other vital interests of Georgia;
b) Executing a mutual assistance request is not in conformity to the requirements established by Georgian legislation;
c) Crime for which mutual assistance is requested, Georgia considers as politically motivated. Offence shall not be considered as politically motivated in case signs of crime prevail to the alleged political motives;
d) Executing a mutual assistance request endangers human rights and fundamental freedoms;
e) Crime for which mutual assistance was requested is of military character and it is not punishable under the legislation of requesting state unless otherwise provided by the International Treaty of Georgia, Individual Agreement or reciprocal conditions;
f) Executing a mutual assistance request violates the principle **non bis in idem (**Double Jeopardy**)**

Article 12 (2) of the same law provides additional requirements for executing mutual assistance request <u>on search and seizure.</u>

These requirements can be summarised as follows:

a) Mutual assistance can only be carried out if the crime for which mutual assistance was requested, is punishable both under Georgian and respective state's legislation;
b) Mutual assistance can only be carried out if the crime for which mutual assistance was requested is subject to extradition possibility;
c) Mutual assistance can only be carried out if it is otherwise in compliance with Georgian legislation.

6.2.12 Germany

Section 59 IRG Admissibility of Assistance

(1) At the request of a competent authority of a foreign State, other legal assistance in a criminal matter may be provided.
(2) Legal assistance within the meaning of subsection (1) above shall be any kind of support given for foreign criminal proceedings regardless of whether the foreign proceedings are conducted by a court or by an executive authority and whether the legal assistance is to be provided by a court or by an executive authority.
(3) Legal assistance may be provided only in those cases in which German courts and executive authorities could render mutual legal assistance to each other.

Section 66 IRG Handing Over of Objects

(1) At the request of a competent authority of a foreign State objects may be handed over
1. which may serve as evidence in foreign proceedings or
2. which the person concerned or an accomplice have obtained for or through the offence on which the request is based,
3. which the person concerned or an accomplice have obtained through the sale of such object or as a replacement for its being destroyed, damaged or taken away or on the basis of a right accrued to them or as usufruct or
4. which were created by or used or meant to be used in the commission or preparation of the offence on which the request is based.

(2) Surrender shall not be admissible unless
1. the offence on which the request is based contains elements of the actus reus and mens rea of a criminal offence or of an offence permitting the imposition of a fine under German law or unless mutatis mutandis it would be such an offence under German law,
2. an order for seizure by a competent authority of the requesting State is submitted or a declaration of such an authority shows that the requirements for seizure would exist if the objects were located in the requesting State and
3. measures are in place to ensure that the rights of third parties will not be infringed and that objects handed over under a condition will be returned upon request without undue delay.

(3) The handing over under subsection (1) nos. 2 to 4 above shall be admissible only as long as no pertinent final and enforceable foreign decision exists with regard to the abovementioned objects.
(4) The public prosecution service at the Landgericht shall prepare the decision about the handing over and shall execute it if granted. The public prosecution service at the Landgericht in whose district the object is located shall have jurisdiction. S. 61(2) 2nd sentence shall apply mutatis mutandis.

Section 94 CCP [Objects Which May Be Seized]

(1) Objects which may be of importance as evidence for the investigation shall be impounded or otherwise secured.
(2) Such objects shall be seized if in the custody of a person and not surrendered voluntarily.
(3) Subsections (1) and (2) shall also apply to driver's licences which are subject to confiscation.

Section 95 CCP [Obligation to Surrender]

(1) A person who has an object of the above-mentioned kind in his custody shall be obliged to produce it and to surrender it upon request.
(2) In the case of non-compliance, the regulatory and coercive measures set out in Section 70 may be used against such person. This shall not apply to persons who are entitled to refuse to testify.

Section 96 CCP [Official Documents]

Submission or surrender of files or other documents officially impounded by authorities or public officials may not be requested if their highest superior authority declares that publication of the content of these files or documents would be detrimental to the welfare of the Federation or of a German *Land*. The first sentence shall apply *mutatis mutandis* to files and other documents held in the custody of a Member of the Federal Parliament or of a *Land* parliament or of an employee of a Federal or *Land* parliamentary group where the agency responsible for authorizing testimony has made a corresponding declaration.

Section 97 CCP [Objects Not Subject to Seizure]

(1) The following objects shall not be subject to seizure:
1. written correspondence between the accused and the persons who, according to Section 52 or Section 53 subsection (1), first sentence, numbers 1 to 3b, may refuse to testify;
2. notes made by the persons specified in Section 53 subsection (1), first sentence, numbers 1 to 3b, concerning confidential information entrusted to them by the accused or concerning other circumstances covered by the right of refusal to testify;
3. other objects, including the findings of medical examinations, which are covered by the right of the persons mentioned in Section 53 subsection (1), first sentence, numbers 1 to 3b, to refuse to testify.
(2) These restrictions shall apply only if these objects are in the custody of a person entitled to refuse to testify unless the object concerned is an electronic health card as defined in section 291a of Part Five of the Social Code. Objects covered by the right of physicians, dentists, psychological psychotherapists, psychotherapists specializing in the treatment of children and juveniles, pharmacists and midwives to refuse to testify shall not be subject to seizure either if they are in the custody of a hospital or a service provider which collects, processes or uses personal data for the persons listed, nor shall objects to which the right of the persons mentioned in Section 53 subsection (1), first sentence, numbers 3a and 3b, to refuse to testify extends, be subject to seizure if they are in the custody of the counselling agency referred to in that provision. The restrictions on seizure shall not apply if certain facts substantiate the suspicion that the person entitled to refuse to testify participated in the criminal offence, or in accessoryship after the fact, obstruction of justice or handling stolen goods, or where the objects concerned have been obtained by means of a criminal offence or have been used or are intended for use in perpetrating a criminal offence, or where they emanate from a criminal offence.
(3) Insofar as the assistants (Section 53a) of the persons mentioned in Section 53a subsection (1), first sentence, numbers 1 to 3b, have a right to refuse to testify, subsections (1) and (2) shall apply *mutatis mutandis*.
(4) The seizure of objects shall be inadmissible insofar as they are covered by the right of the persons mentioned in Section 53 subsection (1), first sentence, number 4, to refuse to testify. This protection from seizure shall also extend to objects which the persons mentioned in Section 53 subsection (1), first sentence, number 4, have entrusted to their assistants (Section 53a). The first sentence shall apply *mutatis mutandis* insofar as the assistants (Section 53a) of the persons mentioned in Section 53 subsection (1), first sentence, number 4, have a right to refuse to testify.
(5) The seizure of documents, sound, image and data media, illustrations and other images in the custody of persons referred to in Section 53 subsection (1), first sentence, number 5, or of the editorial office, the publishing house, the printing works or the broadcasting company, shall be inadmissible insofar as they are covered by the right of such persons to refuse to testify. Subsection (2), third sentence, and Section 160a subsection (4), second sentence, shall apply *mutatis mutandis*; in these cases, too, seizure shall only be admissible, however, where it is not disproportionate to the importance of the case having regard to the basic rights arising out of Article 5 paragraph (1), second sentence, of the Basic Law, and the investigation of the factual circumstances or the establishment of the whereabouts of the perpetrator would otherwise offer no prospect of success or be much more difficult.

Section 98 CCP [Order of Seizure]

(1) Seizure may be ordered only by the court and, in exigent circumstances, by the public prosecution office and the officials assisting it (section 152 of the Courts Constitution Act). Seizure pursuant to Section 97 subsection (5), second sentence, in the premises of an editorial office, publishing house, printing works or broadcasting company may be ordered only by the court.
(2) An official who has seized an object without a court order shall apply for court confirmation within three days if neither the person concerned nor an adult relative was present at the time of seizure, or if the person concerned and, if he was absent, an adult relative of that person expressly objected to the seizure. The person concerned may at any time apply for a court decision. The competence of the court shall be determined by Section 162. The person concerned may also submit the application to the Local Court in whose district the seizure took place, which shall then forward the application to the competent court. The person concerned shall be instructed as to his rights.
(3) Where after public charges have been preferred, the public prosecution office or one of the officials assisting has effected seizure, the court shall be notified of the seizure within three days; the objects seized shall be put at its disposal.
(4) If it is necessary to effect seizure in an official building or an installation of the Federal Armed Forces which is not open to the general public, the superior official agency of the Federal Armed Forces shall be requested to carry out such seizure. The agency making the request shall be entitled to participate. No such request shall be necessary if the seizure is to be made in places which are inhabited exclusively by persons other than members of the Federal Armed Forces.

Section 98a CCP [Automated Comparison and Transmission of Personal Data]

(1) Notwithstanding Sections 94, 110 and 161, where there are sufficient factual indications to show that a criminal offence of substantial significance has been committed
1. relating to the illegal trade in narcotics or weapons or the counterfeiting of money or official stamps,
2. relating to national security (sections 74a, 120 of the Courts Constitution Act),
3. relating to offences which pose a danger to the general public,
4. relating to endangerment of life and limb, sexual self-determination or personal liberty,
5. on a commercial or habitual basis, or
6. by a member of a gang or in some other organized way,

personal data relating to individuals who manifest certain significant features which may be presumed to apply to the perpetrator may be automatically matched against other data in order to exclude individuals who are not under suspicion or to identify individuals who manifest other significant characteristics relevant to the investigations. This measure may be ordered only where other means of establishing the facts or determining the perpetrator's whereabouts would offer much less prospect of success or be much more difficult.
(2) For the purposes of subsection (1), the storing agency shall extract from the database the data required for matching purposes and transmit it to the criminal prosecuting authorities.
(3) Insofar as isolating the data for transmission from other data requires disproportionate effort, the other data shall, upon order, also be transmitted. Their use shall not be admissible.
(4) Upon request by the public prosecution office, the storing agency shall assist the agency effecting the comparison.
(5) Section 95 subsection (2) shall apply *mutatis mutandis*.

Section 98b CCP [Competence; Return and Deletion of Data]

(1) Matching and transmission of data may be ordered only by the court and, in exigent circumstances, also by the public prosecution office. Where the public prosecution office has made the order, it shall request court confirmation without delay. The order shall become ineffective if it is not confirmed by the court within three working days. The order shall be made in writing. It shall name the person obliged to transmit the data and shall be limited to the data and comparison characteristics required for the particular case. The transmission of data may not be ordered where special rules on use, being provisions under Federal law or under the

corresponding *Land* law, present an obstacle to their use. Sections 96 and 97, and Section 98 subsection (1), second sentence, shall apply *mutatis mutandis*.
(2) Regulatory and coercive measures (Section 95 subsection (2)) may be ordered only by the court and, in exigent circumstances, also by the public prosecution office; the imposition of detention shall be reserved to the court.
(3) Where data was transmitted on data media these shall be returned without delay once matching has been completed. Personal data transferred to other data media shall be deleted without delay once it is no longer required for the criminal proceedings.
(4) Upon completion of a measure pursuant to Section 98a, the agency responsible for monitoring compliance with data protection rules by public bodies shall be notified.

Section 98c CCP [Comparison of Data to Clear Up a Criminal Offence]

In order to clear up a criminal offence or to determine the whereabouts of a person sought in connection with criminal proceedings, personal data from criminal proceedings may be automatically matched with other data stored for the purposes of criminal prosecution or execution of sentence, or in order to avert danger. Special rules on use presenting an obstacle thereto, being provisions under Federal law or under the corresponding *Land* law, shall remain unaffected.

Section 99 CCP [Seizure of Postal Items]

Seizure of postal items and telegrams addressed to the accused which are held in the custody of persons or enterprises providing, or collaborating in the provision of, postal or telecommunications services on a commercial basis shall be admissible. Seizure of postal items and telegrams shall also be admissible where known facts support the conclusion that they originate from the accused or are intended for him and that their content is of relevance to the investigation.

Section 100 CCP [Jurisdiction]

(1) Only the court and, in exigent circumstances the public prosecution office, shall be authorized to implement seizure (Section 99).
(2) A seizure ordered by the public prosecution office, even if it has not yet resulted in a delivery, shall become ineffective if it is not confirmed by the court within three working days.
(3) The court shall have the authority to open the delivered post. The court may transfer this authority to the public prosecution office insofar as this is necessary so as not to endanger the success of the investigation by delay. The transfer shall not be contestable; it may be revoked at any time. So long as no order has been made pursuant to the second sentence, the public prosecution office shall immediately forward the delivered postal items to the court, leaving any unopened postal items sealed.
(4) The court competent pursuant to Section 98 shall decide on a seizure ordered by the public prosecution office. The court which ordered or confirmed the seizure shall decide whether to open an item that has been delivered.
(5) Postal items in respect of which no order to open them has been made are to be forwarded to the intended recipient without delay. The same shall apply insofar as there is no necessity to retain the postal items once opened.
(6) Such part of a retained postal item as does not appear expedient to withhold for the purposes of the investigation is to be transmitted to the intended recipient in the form of a copy.

6.2.13 Italy

C.P.P

Art. 696. Prevalenza delle convenzioni e del diritto internazionale generale.

1. Le estradizioni, le rogatorie internazionali, gli effetti delle sentenze penali straniere, l'esecuzione all'estero delle sentenze penali italiane e gli altri rapporti con le autorità straniere, relativi all'amministrazione della giustizia in materia penale, sono disciplinati dalle norme della Convenzione europea di assistenza giudiziaria in materia firmata a Strasburgo il 20 aprile 1959 e dalle altre norme delle convenzioni internazionali in vigore per lo Stato e dalle norme di diritto internazionale generale.
2. Se tali norme mancano o non dispongono diversamente, si applicano le norme che seguono.

Art. 723. Poteri del ministro di grazia e giustizia.

1. Il ministro di grazia e giustizia dispone che si dia corso alla rogatoria di un'autorità straniera per comunicazioni, notificazioni e per attività di acquisizione probatoria, salvo che ritenga che gli atti richiesti compromettano la sovranità, la sicurezza o altri interessi essenziali dello Stato.
2. Il ministro non dà corso alla rogatoria quando risulta evidente che gli atti richiesti sono espressamente vietati dalla legge o sono contrari ai principi fondamentali dell'ordinamento giuridico italiano. Il ministro non dà altresì corso alla rogatoria quando vi sono fondate ragioni per ritenere che considerazioni relative alla razza, alla religione, al sesso, alla nazionalità, alla lingua, alle opinioni politiche o alle condizioni personali o sociali possano influire negativamente sullo svolgimento o sull'esito del processo e non risulta che l'imputato abbia liberamente espresso il suo consenso alla rogatoria.
3. Nei casi in cui la rogatoria ha ad oggetto la citazione di un testimone, di un perito o di un imputato davanti all'autorità giudiziaria straniera, il ministro di grazia e giustizia non dà corso alla rogatoria quando lo Stato richiedente non offre idonea garanzia in ordine all'immunità della persona citata.
4. Il ministro ha inoltre facoltà di non dare corso alla rogatoria quando lo Stato richiedente non dia idonee garanzie di reciprocità.

6.2.14 Japan

Act on International Assistance in Investigation and Other Related Matters

Article 8 (1) With regard to the collection of evidence necessary for assistance, a public prosecutor or a judicial police officer may take the following measures:

(i) To ask any person concerned to appear and interview the person;

(ii) To request an expert opinion;

(iii) To carry out an inspection;

(iv) To request the submission of a document or other material to its owner, possessor or custodian;

(v) To request a public office, or a public or private organization to report on necessary matters;

(vi) To request in writing, a person who engages in the business of providing electronic communication facility for communications of others or a person whose facility for his own electronic communications is capable of transmitting electronic communications among many or unspecified persons to preserve necessary part of the electromagnetic records, which are recorded in the course of business, by specifying the origin, destination, time and other traffic data of the electronic communication for a period not exceeding 30 days (if to extend, not exceeding 60 days in total).

(2) With regard to the collection of evidence necessary for assistance, a public officer or a judicial police officer may, if deemed necessary, undertake seizure, seizure of data medium recorded under an order, search, or inspection of evidence, upon a warrant issued by a judge.

Law n°89 of 2004

Article 3

1. A request for assistance shall be received, and evidence shall be forwarded to the requesting country, by the Minister of Foreign Affairs. The Minister of Justice, however, may carry out these tasks, upon a consent given by the Minister of Foreign Affairs, when a treaty confers the authority to receive requests for assistance on the Minister of Justice, or where exigency or other special circumstances exist.

2. When the Minister of Justice receives a request for assistance or forwards evidence to the requesting country in accordance with the second sentence of the preceding paragraph, the Minister of Justice may ask the Minister of Foreign Affairs for cooperation necessary for the execution of matters relating to the assistance.

Law n°89 of 2004

Article 2

Assistance shall not be provided in any of the following circumstances:
(1) When the offense for which assistance is requested is a political offense, or when the request for assistance is deemed to have been made with a view to investigating a political offense;

(2) Unless otherwise provided by a treaty, when the act constituting the offense for which assistance is requested would not constitute an offense under the laws, regulations or ordinances of Japan were it committed in Japan;

(3) With respect to a request for an examination of a witness or a submission of material evidence, unless otherwise provided by a treaty, when the requesting country does not clearly demonstrate in writing that the evidence is indispensable to the investigation.

Article 4

Upon receiving a request for assistance, the Minister of Foreign Affairs shall, except where any of the following applies, forward the written request for assistance or a certification prepared by the Minister of Foreign Affairs of the fact that such a request has been made , as well as related documents, with the opinion of the Minister of Foreign Affairs attached, to the Minister of Justice:

(1) When a request has been made based on a treaty, where the form of the request does not satisfy the reqirements of the treaty;

(2) When a request has been made without being based on a treaty, where there is no guarantee from the requesting country that it will honor requests of the same sort from Japan.

Article 15

When the Minister of Justice, after taking measures as provided for in paragraph l, item (2) or (3) of Article 5, or in paragraph 2 of Article 5, deems it to be inappropriate to provide assistance, he/she shall, without delay, notify the person who has received the documents concerning the request for assistance to that effect.

6.2.15 Latvia

Criminal procedure law

Article 845. - Grounds for the Assistance to a Foreign State in the Performance of Procedural actions

The following are grounds for procedural assistance:
1) a request of a foreign state regarding the provision of assistance in the performance of a procedural action;
2) a decision of a competent authority of Latvia regarding the admissibility of a procedural action.

6.2.16 Lithuania

Article 6 Paragraph 3 of the Law on Police Activities of the Republic of Lithuania

"The police may provide data, in the manner prescribed by legislation of the European Union, international treaties and other legal acts of the Republic of Lithuania, to law enforcement agencies of foreign states as well as to international law enforcement organisations for the purposes of detection, investigation and prevention of criminal acts, ensuring of public order, rendering of emergency assistance to persons when it is necessary because of their physical or mental helplessness, as well as to persons who have suffered from criminal acts, other violations of law, natural calamities or similar acts." (Law No. XI-444, 22 October 2009, entered into force since 31 October 2009, Official Gazette, No. 130-5637, 2009).

Criminal Code of the RL

Article 119. Espionage

1. A person who, for the purpose of communicating it to a foreign state or organisation thereof, seizes, purchases or otherwise collects the information constituting a state secret of the Republic of Lithuania or communicates this information to a foreign state, organisation thereof or their representative
shall be punished by imprisonment for a term of two up to ten years.
2. A person who, in performing an assignment of another state or organisation thereof, seizes, purchases or otherwise collects or communicates the information constituting a state secret of the Republic of Lithuania or another information of interest to the intelligence of a foreign state
shall be punished by imprisonment for a term of three up to fifteen years.

Article 124. Unlawful Possession of the Information Constituting a State Secret

A person who unlawfully acquires or conveys the information constituting a state secret of the Republic of Lithuania or unlawfully holds in possession the material items whose content or information thereon constitutes a state secret of the Republic of Lithuania, in the absence of characteristics of espionage,
shall be punished by a fine or by arrest or by imprisonment for a term of up to three years.

Article 125. Disclosure of a State Secret

1. A person who discloses the information constituting a state secret of the Republic of Lithuania, where this information was entrusted to him or he gained access thereto through his service, work or in the course of performance of public functions, but in the absence of characteristics of espionage,
shall be punished by deprivation of the right to be employed in a certain position or to engage in a certain type of activities or by imprisonment for a term of up to three years.
2. The act provided for in paragraph 1 of this Article shall be a crime also where it has been committed through negligence.

Article 166. Violation of Inviolability of a Person's Correspondence

1. A person who unlawfully intercepts a postal item or package sent by post or via a provider of courier services or unlawfully intercepts, records or observes a person's messages transmitted by electronic communications networks or unlawfully records, wiretaps or observes a person's conversations transmitted by electronic communications networks or otherwise violates inviolability of a person's correspondence
shall be punished by community service or by a fine or by restriction of liberty or by arrest or by imprisonment for a term of up to two year.
2. A legal entity shall also be held liable for an act provided for in this Article.

Article 167. Unlawful Collection of Information about a Person's Private Life

1. A person who unlawfully collects information about a person's private life shall be punished by community service or by a fine or by restriction of liberty or by arrest or by imprisonment for a term of up to three years.
2. A legal entity shall also be held liable for an act provided for in this Article.

Article 168. Unauthorised Disclosure or Use of Information about a Person's Private Life

1. A person who, without another person's consent, makes public, uses for his own benefit or for the benefit of another person information about the private life of another person, where he gains access to that information through his service or profession or in the course of performance of a temporary assignment or he collects it through the commission of an act provided for in Articles 165-167 of this Code,
shall be punished by community service or by a fine or by restriction of liberty or by arrest or by imprisonment for a term of up to three years.
2. A legal entity shall also be held liable for an act provided for in this Article.
3. A person shall be held liable for an act provided for in this Article only subject to a complaint filed by the victim or a statement by his authorised representative or at the prosecutor's request.

Article 210. Commercial Espionage

A person who unlawfully acquires the information considered to be a commercial secret or communicates this information to another person
shall be punished by deprivation of the right to be employed in a certain position or to engage in a certain type of activities or by restriction of liberty or by arrest or by imprisonment for a term of up to two years.

Article 211. Disclosure of a Commercial Secret

A person who discloses the information considered to be a commercial secret which was entrusted to him or which he accessed through his service or work, where this act incurs major property damage to the victim,
shall be punished by deprivation of the right to be employed in a certain position or to engage in a certain type of activities or by a fine or by restriction of liberty or by arrest or by imprisonment for a term of up to two years.

Article 296. Seizure or Other Unlawful Acquisition of an Official Secret

A person who seizes, purchases or otherwise unlawfully acquires a material item whose content or information thereon constitutes an official secret or transfers the item or information thus acquired to a third party, in the absence of characteristics of espionage or provision of assistance to a foreign state, shall be punished by a fine or by arrest or by imprisonment for a term of up to two years.

Article 297. Disclosure of an Official Secret

1. A person who discloses the information constituting an official secret which was entrusted to him or which he accessed through his service or work, in the absence of characteristics of espionage or assistance to a foreign state in carrying out activities hostile to the Republic of Lithuania, shall be considered to have committed a misdemeanour and shall be punished by deprivation of the right to be employed in a certain position or to engage in a certain type of activities or by a fine or by restriction of liberty.
2. The act provided for in this Article shall be considered as criminal also where it has been committed through negligence."

6.2.17 Moldova

Criminal Procedure Code of the Republic of Moldova

Article 531. Legal regulation of international legal assistance

(1) Relations with foreign countries or international courts on legal assistance in criminal matters are covered in this chapter and the provisions of the Law on International Legal Assistance in Criminal Matters. Provisions of international treaties to which Moldova is a party and other international obligations of the Republic of Moldova will have precedence over the provisions of this chapter.

(2) If the Republic of Moldova is party to several international legal instruments to which the State is a party to legal assistance is requested or the requesting State and divergences arise between the rules of such acts or inconsistencies, the provisions of the treaty that provides beneficial protection of human rights and freedoms.

(3) Ministry of Justice can decide to not execute a court decision on the admission of international legal assistance in case of the fundamental national interests are disputable. This task is exercised fully to respect the rights of litigants in the execution of judgments in their favor.

Article 534. Refusal to international legal assistance

(1) International legal assistance may be refused if:

1) the request relates to offenses considered in the Republic of Moldova as political offenses or offenses connected with such crimes. Refusal is not admissible if the person is suspected, accused or sentenced for the committing of offenses under article 5-8 from the Rome Statute of the International Criminal Court;
2) the request concerns an offense which is solely a violation of military discipline;
3) the requested for legal assistance criminal prosecution body or court consider that execution likely to prejudice the sovereignty, security or public policy of the state;
4) there are reasonable grounds to believe that the suspect is criminally prosecuted or punished on account of race, religion, nationality, association with a particular group or political beliefs, shared, or if his situation will further aggravate for listed grounds;
5) it is proved that the person in requesting state will not have access to a fair trial;
6) the respective offense is punishable with death under the law of the requesting State and the requesting State gives no warranty for non-application or non-performance penalty;
7) under the Criminal Code of the Republic of Moldova, the invoked in the request offense or offenses are not an offense;
8) in accordance with national law, a person can not be held to criminal liability.

(2) Any refusal on international legal assistance will be motivated.

Article 536. Addressing the letter rogatory

(1) The criminal prosecution body or the court, if considered necessary making a procedural action in a foreign state, letters rogatory addressed by the criminal investigation body or the court of that State or an international criminal court under international treaty to which Moldova is a party or by diplomatic means, in terms of reciprocity.

(2) Conditions of reciprocity is confirmed in a letter that the Minister of Justice and General Prosecutor undertakes to grant, on behalf of the Republic of Moldova, legal assistance to foreign state or to international criminal court conducting procedural actions, guaranteeing procedural rights provided by national law of the person against whom assistance is made.

(3) Rogatory commission in the Republic of Moldova shall be submitted by the prosecution to the General Prosecutor and by the court - Minister of Justice submission for execution to the respectove state.

(4) A demand of rogatory commission and attached documents shall be drawn up in the official language and are translated into the language of requested State or in another language, according to provisions or reserves to applicable international treaty.

Article 537

(1) The request for the rogatory commission shall be done in writing and must include:

1) name of the body that addresses with the request;

2) name and address, if known, of the institution to which the request is sent;

3) international treaty or reciprocal agreement under which assistance is requested;

4) indicate criminal case in which is requested legal assistance, information about facts that have committed their actions and the legal text article of the Criminal Code of the Republic of Moldova and data on the damage caused by the offense;

5) data on persons who requested the rogatory commission, including their procedural capacity, date and place of birth, citizenship, residence, occupation, for legal entities - their name and address and the name and addresses of their representatives people when necessary;

6) the claim and data necessary to carry them with exposure circumstances which will be found, the list of documents, material evidence and other evidence requested, the circumstances on which the test is to be administered and the questions that need to be made to persons to be heard.

7) the date which is expected to reply to the request and, where appropriate, a request to allow the execution respective procedural actions to assist the criminal investigation body representative of the Republic of Moldova.

(1^1) at the rogatory commission request is attached the procedural acts necessary to carry out criminal actions, prepared in accordance with the provisions of this Code.

(2) The request for rogatory commission and the attached documents are signed and authenticated by the official stamp of the competent institution demanding.

Article 538.

Validity procedural act Procedural document issued in a foreign country in accordance with the law of that country applies to the prosecuting authorities and the courts of the Republic of Moldova.

Article 539. Quoting witnesses, experts or people being pursued over outside the Republic of Moldova

(1) A witness, expert or prosecuted person, if that is not search time, are outside Moldova may be called by the prosecution to perform certain procedural actions in Moldova. In this case, the summons can not contain injunction forced to bring into the law enforcement body.

(2) summoning the witness or expert shall be as provided in art.536 par. (3) and (4).

(3) actions with the participation of persons summoned under this Article shall be made under this Code.

(4) A witness, expert or prosecuted person, regardless of their nationality, who appeared before the body that has requested following a summons under this Article shall not be prosecuted or detained or subjected to any other restriction of freedom their individual Moldovan territory for acts or convictions anterior border of the Republic of Moldova.

(5) The immunity provided in par. (4) ceases if the person cited has not left the territory of the Republic of Moldova within 15 days of the date on which organ called her/his and informed him that his presence is no longer required and then returned to Moldova. In this term does not include the time the person cited could not leave Moldova for reasons beyond his control.

(6) Citation detainee in a foreign state shall be made under this Article, provided that the person temporarily transferred in Moldova by the respective authority of the foreign country to perform the actions

specified in the request for transfer will be returned within the time stated in request. Conditions of transfer or refusal of transfer is regulated by international treaties to which the Republic of Moldova and the requested country are part of or pursuant to obligations under the mutual written.

(7) A witness or expert quoted is entitled to demand reimbursement of expenses for travel, accommodation and subsistence expenses incurred in connection with absence from work reasons.

(8) The witness heard under this article shall, as appropriate, beneficiate of protection under the law.

Article 540[1]. Search, collection, remittance objects or documents, seizure and confiscation

Rogatory commission requesting a search, increasing or remission of objects or documents, as well as seizure or confiscation are executed in accordance with the legislation of the Republic of Moldova.

Article 540. Execution in Moldova of the rogatory commission required by foreign authorities

(1) The criminal prosecution body or the court executed the requested rogatory commission by foreign bodies such under international treaties to which the Republic of Moldova and the applicant are partially or reciprocal confirmed according to art.536 par. (2).

(2) The request for rogatory commission shall be sent by the General Prosecutor Office to the criminal investigation body or, where appropriate, by the Ministry of Justice to the court of the place where they are to be carried procedural action required.

(4) At the execution of the rogatory commission, the provisions of this code, however, at the request of the requesting Party may apply a special procedure under the law of the foreign country in accordance with international treaty itself or on condition of reciprocity, unless it conflicts with national and international obligations of the Republic of Moldova.

(5) At the execution of the rogatory commission, can assist representatives from foreign state or international court if it is stipulated by an international treaty or a question written on a reciprocal obligation. In this case, at the request of the applicant, the body entrusted with the execution of the rogatory commission informs the requesting Party of the time, place and time of execution of the rogatory commission in order that interested parties can attend.

(6) If the person against whom enforcement is sought is indicated wrong rogatory commission, the body entrusted with the execution of the measures in order to determine the address. If address setting is not possible, notify the applicant about it.

(7) In case if the rogatory commission request may not be executed, documents received shall be returned to the requesting Party through the institutions from which they received, and the reasons that prevented execution. Request of rogatory commission and attached documents shall be returned and in case of refusal on the grounds provided in art.534.

Article540[2]. Joint investigation teams

(1) The competent authorities of two or more states may constitute agreement, a joint investigation team for a specific purpose and for a limited period may be extended by mutual consent, to conduct a criminal investigation or in several of the states that constitute the team. Joint investigation team composition is decided by mutual agreement.

(2) Joint investigation teams can be created when:

1) In a prosecution pending in the requesting State should be carried out difficult prosecutions involving mobilization of substantial resources regarding other states;

2) More States are conducting criminal investigations that require coordinated, concerted action in those countries.

(3) Demand for training joint investigation team may be made by any state involved. Joint investigation team is formed in one of the States to be made criminal.

(4) Demand for training joint investigation team comprising authority which made the request, subject and reason for the request, the identity and nationality of the person, name and address, if applicable, and its proposals for the composition.

(5) Components joint investigation team appointed by Moldovan authorities as members, while members appointed by a foreign state are members posted.

(6) Joint investigation team's work in Moldova is carried out according to the following rules:

1) Joint investigation team leader is a representative of the authority participating in criminal proceedings in the Member State in whose territory the team and act within its powers under its national;

2) the team shall carry out the law of the Republic of Moldova. Team members and seconded members perform their tasks under the responsibility of the person referred to in section 1), taking into account the conditions set by their own authorities in the agreement on team building.

(7) Seconded members beside joint investigation teams are entitled to attend any procedural, unless the team leader, for special reasons decides otherwise.

(8) When joint investigation team is to perform procedural acts in that State, seconded members may request their own competent authorities to take those measures.

(9) A member of the next joint investigation team may, under its national law and its powers are to provide information to the team that posted the state in the purpose of the prosecution.

(10) Information lawfully obtained by a member or seconded member while part of a joint investigation team that can not be obtained otherwise by the competent authorities of the states concerned may be used:

1) the purpose for which it was created team;
2) for discovering, investigating and prosecuting other criminal offenses with the consent of the state in which the information was obtained;
3) for preventing an immediate and serious threat to public security, respecting the provisions of section 2);
4) other purposes, if it is agreed by states formed team.

(11) In case of joint investigation teams operating in the republic of Moldova, seconded members of the team are treated as members of the Republic of Moldova regarding crimes committed against them or by them.

6.2.18 Montenegro

Law on International Legal Assistance in Criminal Matters

Article 3

International legal assistance shall include extradition of the accused and sentenced persons, transfer and assuming of criminal prosecution, enforcement of foreign criminal verdicts, delivery of documents, writs and other cases associated with the criminal proceedings in the requesting state, as well as the undertaking of certain procedural actions such as: hearing of the accused, witnesses and experts, crime scene investigation, search of premises and persons and temporary seizure of items.

Article 4

The Ministry responsible for the judiciary (hereinafter referred to as the Ministry) shall be a central communication authority through which domestic judicial authorities shall forward letters rogatory for international legal assistance to foreign judicial authorities and vice versa.
In cases when this has been provided for under an international agreement or where there is reciprocity, the Ministry shall submit letters rogatory to the central communication authority of the requested state, and in cases where there is no such agreement or reciprocity, the Ministry shall deliver and receive letters rogatory for international legal assistance through diplomatic channels.
Without prejudice to the above, if provided for under an international agreement, domestic judicial authorities may deliver letters rogatory for international legal assistance to a foreign judicial authority directly and they shall be obliged to deliver the copy of the letter rogatory to the Ministry.
In urgent cases, provided that there is reciprocity, letter rogatory for international legal assistance may be delivered through the National Central Bureau – INTERPOL.
The higher court and the state prosecutor shall be responsible for provision of international legal assistance in accordance with the law.

Article 5

The Ministry shall deliver, without delay, the letters rogatory from foreign judicial authorities to domestic judicial authorities, except in cases when it is obvious that the letter rogatory should be rejected.
The permissibility and the method of enforcement of the action which is the subject matter of a foreign judicial authority shall be decided by the court in accordance with domestic legislation and ratified international agreements.

Article 6

The basis for provision of international criminal assistance shall be that the offence for which the provision of international legal assistance is requested is a criminal offence both under the domestic law and under the law of the requesting country the judicial authority of which presented the letter rogatory

Article 7

Unless otherwise has been provided for by an international agreement or this Law, signed and certified letter rogatory for international legal assistance shall contain:

1) the name and the seat of the authority making the request;
2) the name of the requested authority, and if its precise name is unknown, an indication that the letter rogatory is being sent to the competent judicial authority, and the name of the country;
3) legal basis for the provision of international legal assistance;

4) the form of the international legal assistance requested and the reason for the letter rogatory;
5) legal qualification of the criminal offence committed and the summary of the facts, except if the letter rogatory refers to the service of court writs (applications, documents and the like);
6) nationality and other personal details of the person regarding which the international legal assistance is requested and his status in the proceedings;
7) in case of service of court writs, their type.

6.2.19 Netherlands

Articles 552h to 552s and Articles 552jj to 552vv of the Dutch Code of Criminal Procedure (DCCP) shall be taken into account.

Article 552(h) DCCP provides that the title relates to the requests for mutual legal assistance that have been made in connection with a criminal case. So, there have to be foreign criminal proceedings in the investigation, prosecution, handling in court and execution phase. The crimes committed must be punishable according to the law of the requesting state. Since a coercive measure has to be applied in the territory of the Netherlands, i.e. obtaining stored data, the act should be punishable under Dutch law. Furthermore, this criminal offence should be listed in Article 67 DCCP, which sums up offences for which pre-trial detention is allowed.
Extract Criminal Procedure Code:
http://www.wetboek-online.nl/wet/Wetboek%20van%20Strafvordering.html#3857, select "Titel X. Internationale Rechtshulp"

6.2.20 Norway

Norwegian Criminal Procedure Act does not have specific regulation of cooperation with law enforcement in other jurisdictions. Article 215a (expedited preservation of data) does refer to request from other countries as a possible background for expedited preservation.

Norwegian Courts of Justice Act, Article 46, first subsection, Norwegian courts can only process a request from courts or authorities in other countries if the request is sent through the relevant Norwegian Ministry (The Ministry of Justice), unless otherwise is stated.

6.2.21 Portugal

Cybercrime Law - Law nr 109/2009

Article 20 - International cooperation

The national authorities shall cooperate with the competent foreign authorities for the purpose of criminal investigations or proceedings relating computer systems or data, as well as the collection of evidence of a crime in electronic form, according to the rules on transfer of personal data contained in Law No 67/98 of 26 October.

Article 22 - Preservation and expedited disclosure of computer data within international cooperation

1 – Portugal may be requested to expedite preservation of data stored in a computer system located in the country, referring to crimes described under Article 11, in view to submit a request for assistance for search, seizure and disclosure of those data.
2 - The request specifies:
a) the authority requesting the preservation;
b) that the offense is being investigated or prosecuted, as well as a brief statement of the facts relating thereto;
c) the computer data to be retained and its relation to the offense;
d) all the available information to identify the person responsible for the data or the location of the computer system;
e) the necessity of the measure of preservation, and
f) The intention to submit a request for assistance for search, seizure and disclosure of the data.
3 – Executing the demand of a foreign authority under the preceding paragraphs, the competent judicial authority orders the person who has the control or availability of such data, including a service provider, to preserve them.
4 - Preservation can also be ordered by *Polícia Judiciária*, after authorization obtained from the competent judicial authority or when there is emergency or danger in delay; in this case it is applicable, paragraph 4 of the preceding article.
5 - A preservation order specifies, on penalty of nullity:
a) the nature of the data;
b) if known, the source and their destination, and
c) the period of time during which that data must be preserved for up to three months.
6 - In compliance with the addressed preservation order, who has the control or availability of such data, including a service provider, preserves immediately the data by the specified period of time, protecting and maintaining its integrity.
7 - The competent judicial authority, or *Policia Judiciária* with permission of the judicial authority, may order the renewal of the measure for periods subject to the limit specified in item c) of paragraph 5, provided they meet the respective requirements of admissibility, to the maximum a year.
8 - When the request referred to in paragraph 1 is received, the competent judicial authority decides the preservation of data until the adoption of a final decision on the request.
9 - Data preserved under this Article may only be provided:
a) to the competent judicial authority, in the execution of the application for cooperation referred to in paragraph 1, in the same way that it could have been done in a similar national case, under Articles 13 to 17;
b) to the national authority which issued the order to preserve, in the same way that it could have been done, in a similar national case under Article 13.
10 - The national authority that, under the preceding paragraph, receives traffic data identifying intermediate service providers by which the communication was made, quickly communicates this fact to the requesting authority in order to enable this authority to submit to the competent authority another request for expedited preservation of data.
11 – The provisions of paragraphs 1 and 2 shall apply, *mutatis mutandis*, to requests sent to other authorities by the Portuguese authorities.

Article 23 - Grounds for refusal

1 - A request for expedited preservation or disclosure of computer data is refused if:
a) the computer data in question refer to a political offense or a related offense according to Portuguese law;
b) it attempts against the sovereignty, security, *ordre publique* or other constitutionally defined interests of the Portuguese Republic;
c) the requesting State does not provide guarantees for the protection of personal data.
2 - A request for expedited preservation of computer data can still be refused if there are reasonable grounds to believe that the execution of a request for legal assistance for subsequent search, seizure and release of such data shall be denied for lack of verification of dual criminality.

Article 24 - Access to computer data within international cooperation

1 – In the execution of the request of the foreign authority, the competent judicial authority may proceed with the search, seizure and disclosure of data stored in the computer system located in Portugal, related to crimes defined in Article 11, when the search and seizure would be admissible in a similar national case.
2 - The judicial authority shall proceed as quickly as possible when there is reason to believe that the computer data in question are particularly vulnerable to loss or modification, or where cooperation is provided for an expedited instrument of cooperation described in any international legal instrument.
3 - The provisions of paragraph 1 shall apply, *mutatis mutandis*, to requests made by Portuguese judicial authorities.

Article 25 - Cross-border access to computer data stored when publicly available or with consent
The competent foreign authorities without prior request from the Portuguese authorities, in accordance with the rules on transfer of personal data provided by Law No. 67/98 of 26 October, may:
a) access data stored in a computer system located in Portugal, where publicly available;
b) receive or access through a computer system located in its territory, the data stored in Portugal, through legal and voluntary consent of the person legally authorized to disclose them.

Article 26 - Interception of communications within international cooperation
1 - Pursuant to a request by the competent foreign authority it may be authorized by the judge the interception of computer data transmissions from a computer system located in Portugal, since it is stipulated by a treaty or an international agreement and whether it is a case where such interception is allowed under Article 18, in a similar national case.
2 – *Policia Judiciária* is the responsible entity for receiving requests to intercept communications, which report to the Public Prosecution Service, so as they can be presented to the judge in charge of the *comarca* of Lisbon for authorization.
3 - The referred order of authorization also allows the immediate transmission of the communication to the requesting State, if such a procedure is foreseen in a treaty or an international agreement under which the request is made.
4 - The provisions of paragraph 1 shall apply, *mutatis mutandis*, to requests made by Portuguese judicial authorities.

Article 145-A of the general framework of the judicial cooperation (Law Nr 144/99, of 31 August, as amended by Laws Nr 104/2001, of 25 August, Law Nr 48/2003, of 22 August, Law Nr 48/2007 of 29 August and Law Nr 115/2009 of 12 October - Law on International Judicial Co-operation in Criminal Matters)

6.2.22 Romania

L302/2004 (Article 11 - Direct transmission)

(1) Requests for international judicial assistance in criminal maaters may be sent directly by the requesting judicial authorities to the requested judicial authorities if the international judicial instrument applicable in the relation between the Requesting State and the Requested State regulates this type of transmission.
(2) With the exception of the case mentioned in para.(1), requests for international judicial assistance can be sent directly by the requesting judicial authorities to the requested judicial authorities in case of emergency; however, a copy of these shall be sent simultaneously to the Ministry of Justice or to the Public Prosecutor's Office attached to the High Court of Cassation and Justice, according to case.
(3) The procedure mentioned in para.(1) and (2) shall be used also for transmitting replies to emergency requests for judicial assistance.
(4) In the case under para. (1) and (2), direct transmissions can be made through the International Criminal Police Organisation (Interpol).

ARTICLE 12 - Other modalities of sending the requests

(1) In order to send requests, based on the agreement between the Requesting and the Requested States, adequate electronic means may be used as well, in particular fax, when available, if the authenticity and confidentiality of the request, as well as the credibility of the data sent are guaranteed.
(2) The previous paragraph shall not prevent the use of the emergency means provided in Article 11.

- Law no. 302/2004 on International Judicial Cooperation in Criminal Matters (republished)
- Law No. 161/2003 Title III (The Prevention and Countering of Cyber-Crime)
- Law no. 508/ 2004 on the Creation, Organization and Operation of the Directorate for Investigating Organized Crime and Terrorism
- Law 39/2003 on the Prevention and Combating of Organized Crime
- Law 656/2002 on the Prevention and Sanctioning of Money Laundering

Article 8 (Non bis in idem) of the Law no 302/2004 provides that international judicial cooperation is not admissible when, in Romania or in any other State, criminal prosecution has taken place for the same act and if:
a) a final jugement stated the acquittal or ceasing of the criminal trial;
b) the penalty imposed through a final sentence has been served or was subject to a pardon or amnesty, either as a whole or a the part of it;
(2) Paragraph (1) shall not apply if assistance is requested in order to review the final decision, for one of the reasons that justify the promotion of a means of extraordinary judicial appeal provided in the Romanian Criminal Procedure Code.
(3) Paragraph (1) shall not apply where an international treaty to which Romania is part of contains conditions that are more favourable as regards the principle of non bis in idem.

6.2.23 Serbia

Law on Mutual Assistance In Criminal Matters of Republic of Serbia

Article 7

1) The criminal offence, in respect of which legal assistance is requested, constitutes the offence under the legislation of the Republic of Serbia;
2) The proceedings on the same offence have not been fully completed before the national court, that is, a criminal sanction has not been fully executed;
3) The criminal prosecution, that is, the execution of a criminal sanction is not excluded due to the state of limitations, amnesty or an ordinary pardon;
4) The request for legal assistance does not refer to a political offence or an offence relating to a political offence, that is, a criminal offence comprising solely violation of military duties;
5) The execution of requests for mutual assistance would not infringe sovereignty, security, public order or other interests of essential significance for the Republic of Serbia.

List of the grounds for refusal of request for MLA according **to Law on Mutual Assistance in Criminal Matters**:

1) the criminal offence, in respect of which legal assistance is requested, doesn`t constitute the offence under the legislation of the Republic of Serbia;
2) the proceedings on the same offence have been fully completed before the national court, that is, a criminal sanction has been fully executed;
3) the criminal prosecution, that is, the execution of a criminal sanction is excluded due to the state of limitations, amnesty or an ordinary pardon;
4) the request for legal assistance refer to a political offence or an offence relating to a political offence, that is, a criminal offence comprising solely violation of military duties;
5) the execution of requests for mutual assistance would infringe sovereignty, security, public order or other interests of essential significance for the Republic of Serbia.

6.2.24 Slovakia

Code of Criminal Procedure	Trestný priadok
Letters Rogatory of Foreign Authorities	**Dožiadania cudzích orgánov**
Section 537 **Method and Form of Letters Rogatory Processing**	**§ 537** **Spôsob a forma vybavenia dožiadania**
(1) The Slovak authorities shall perform the legal assistance requested by the foreign authorities in the manner regulated by this Act or an international treaty. If legal assistance is provided under an international treaty in a manner which is not governed by this Act, the competent public prosecutor shall decide in what manner the legal assistance should be performed.	(1) Slovenské orgány vykonávajú právnu pomoc požadovanú cudzími orgánmi spôsobom upraveným v tomto zákone alebo v medzinárodnej zmluve. Ak sa poskytuje právna pomoc podľa medzinárodnej zmluvy postupom, ktorý nie je upravený v tomto zákone, rozhodne príslušný prokurátor, akým spôsobom sa právna pomoc vykoná.
(2) The requested legal assistance may be performed upon the request of a foreign authority under a legal regulation of the requesting State, if the requested procedure is not contrary to the interests protected by the provisions of Section 481.	(2) Na žiadosť cudzieho orgánu možno požadovanú právnu pomoc vykonať podľa právneho predpisu dožadujúceho štátu, ak žiadaný postup nie je v rozpore so záujmami chránenými ustanovením § 481.
(3) For the performance of letters rogatory under Section 539 Subsection 1, it is requested that the act, which the letters rogatory concern, is a criminal offence not only under the legal system of the requesting State, but also the legal system of the Slovak Republic.	(3) Na vykonanie dožiadania podľa § 539 ods. 1 sa vyžaduje, aby čin, ktorého sa dožiadanie týka, bol trestným činom nielen podľa právneho poriadku dožadujúceho štátu, ale aj právneho poriadku Slovenskej republiky.
Section 538 **Jurisdiction for the Processing of Letters Rogatory**	§ 538 **Príslušnosť na vybavenie dožiadania**
(1) The letters rogatory of a foreign authority for legal assistance shall be served to the Ministry of Justice.	(1) Dožiadania cudzieho orgánu o právnu pomoc sa zasielajú ministerstvu spravodlivosti.
(2) To ensure the processing of a letter rogatory from a foreign authority for legal assistance, the district prosecution, under which jurisdiction the requested act of legal assistance is to be performed, is competent. If the local jurisdiction is given to several public prosecutions, the Ministry of Justice shall send the letters rogatory to the Attorney General's Office for a decision as to which of the public prosecutions shall provide its processing.	(2) Na zabezpečenie vybavenia dožiadania cudzieho orgánu o právnu pomoc je príslušná okresná prokuratúra, v ktorej obvode sa požadovaný úkon právnej pomoci má vykonať. Ak je daná miestna príslušnosť viacerých prokuratúr, zašle ministerstvo spravodlivosti dožiadanie generálnej prokuratúre na rozhodnutie, ktorá prokuratúra zabezpečí jeho vybavenie.
(3) If a foreign authority requests the performance of an interrogation or another act of legal assistance by the court due to the application of the act in the criminal proceedings in the requesting State, the public prosecutor shall submit the letters rogatory of a foreign authority to this extent to the District Court under which jurisdiction the act of legal assistance is to be performed, for processing. If the subject of the letters rogatory is solely an act which is to be performed by the court, the Ministry of Justice shall serve the request directly to the competent court.	(3) Ak cudzí orgán požiada o vykonanie výsluchu alebo iného úkonu právnej pomoci súdom z dôvodu použiteľnosti úkonu v trestnom konaní v dožadujúcom štáte, predloží prokurátor v tejto časti dožiadanie cudzieho orgánu na vybavenie okresnému súdu, v ktorého obvode sa úkon právnej pomoci má vykonať. Ak predmetom dožiadania je výlučne úkon, ktorý má vykonať súd, zašle ministerstvo spravodlivosti dožiadanie priamo príslušnému súdu.
Section 539 **Permission of an Act of Legal Assistance for the Courts**	**§ 539** **Povolenie úkonu právnej pomoci súdom**
(1) If the order of the court under this Act is necessary for the performance of evidence requested by a foreign authority, the court shall issue an order upon the petition of the public prosecutor providing the processing of the letters rogatory.	(1) Ak sa podľa tohto zákona vyžaduje na vykonanie dôkazu požadovaného cudzím orgánom príkaz súdu, vydá príkaz súd na návrh prokurátora zabezpečujúceho vybavenie dožiadania.
(2) If the act of legal assistance is to be performed under a foreign regulation, the court shall decide, upon the petition of the public prosecutor, whether the procedure under the foreign regulation is not contrary to the interests protected by the provisions of Section 481. If they do not find such conflict, the act shall be permitted and they shall simultaneously decide on the manner of its performance. The public prosecutor may file a complaint against the decision of the court, which has a suspensive effect. The decision of the court on the conflict of the procedure under a	(2) Ak sa úkon právnej pomoci má vykonať podľa cudzieho predpisu, rozhodne súd na návrh prokurátora, či postup podľa cudzieho predpisu nie je v rozpore so záujmami chránenými ustanovením § 481. Ak takýto rozpor nezistí, úkon povolí a súčasne rozhodne, akým spôsobom sa vykoná. Proti rozhodnutiu súdu môže prokurátor podať sťažnosť, ktorá má odkladný účinok. Rozhodnutie súdu o rozpore postupu podľa cudzieho predpisu sa nevyžaduje, ak ide o doručenie písomnosti alebo poučenie osoby podľa

foreign regulation shall not be required if it is a serving of documents or instruction of the person under a foreign regulation. (3) The District Court under which jurisdiction the act of legal assistance is to be performed is competent to make a decision under Subsection 1 and 2.	cudzieho predpisu. (3) Na rozhodnutie podľa odsekov 1 a 2 je príslušný okresný súd, v ktorého obvode sa úkon právnej pomoci má vykonať.

Section 90 of the Code of Criminal Procedure **Preservation and Disclosure of Computer Data**	**§ 90 Trestného poriadku** **Uchovanie a vydanie počítačových údajov**
(1) If the preservation of the stored computer data is necessary for the clarification of the facts necessary for the criminal proceedings, including traffic data that is stored through a computer system, the presiding judge and, before the initiation of the criminal prosecution or in the preliminary hearing, the public prosecutor, may issue an order that must be justified even by the merits, to the person who possesses or controls such data, or the provider of such services to	(1) Ak je na objasnenie skutočností závažných pre trestné konanie nevyhnutné uchovanie uložených počítačových údajov vrátane prevádzkových údajov, ktoré boli uložené prostredníctvom počítačového systému, môže predseda senátu a pred začatím trestného stíhania alebo v prípravnom konaní prokurátor vydať príkaz, ktorý musí byť odôvodnený aj skutkovými okolnosťami, osobe, v ktorej držbe alebo pod jej kontrolou sa nachádzajú také údaje, alebo poskytovateľovi takých služieb, aby
a) store such data and maintain the integrity thereof,	a) také údaje uchovali a udržiavali v celistvosti,
b) allow the production or retention of a copy of such data,	b) umožnili vyhotovenie a ponechanie si kópie takých údajov,
c) render access to such data impossible,	c) znemožnili prístup k takým údajom,
d) remove such data from the computer system,	d) také údaje odstránili z počítačového systému,
e) release such data for the purposes of the criminal proceedings.	e) také údaje vydali na účely trestného konania.
(2) In the order under Subsection 1 Paragraphs a) or c), a period during which the data storage shall be performed must be determined. This period may be up to 90 days, and if its re-storage is necessary, a new order must be issued.	(2) V príkaze podľa odseku 1 musí byť ustanovený čas, po ktorý bude uchovávanie údajov vykonávané, tento čas môže byť až na 90 dní, a ak je potrebné ich opätovné uchovanie, musí byť vydaný nový príkaz.
(3) If the storage of the computer data, including the traffic data for the purpose of the criminal proceedings, is no longer necessary, the presiding judge and, before the onset of the criminal prosecution or in the preliminary hearing, the public prosecutor, shall issue an order for the revocation of the storage of such data without undue delay.	(3) Ak uchovávanie počítačových údajov vrátane prevádzkových údajov na účely trestného konania už nie je potrebné, vydá predseda senátu a pred začatím trestného stíhania alebo v prípravnom konaní prokurátor bez meškania príkaz na zrušenie uchovávania týchto údajov.
(4) The order under Subsection 1 through 3 shall be served to the person who possesses or controls such data, or to the provider of such services, and they may be imposed an obligation to maintain the confidentiality of the measures specified in the order.	(4) Príkaz podľa odsekov 1 až 3 sa doručí osobe, v ktorej držbe alebo pod jej kontrolou sa nachádzajú také údaje, alebo poskytovateľovi takých služieb, ktorým sa môže uložiť povinnosť zachovať v tajnosti opatrenia uvedené v príkaze.
(5) The person who possesses or controls the computer data shall release such data or the provider of services shall issue the information regarding the services that are in their possession or under their control to those who issued the order under Subsection 1 or to the person referred to in the order under Subsection 1.	(5) Osoba, v ktorej držbe alebo pod jej kontrolou sa nachádzajú počítačové údaje, vydá tieto údaje, alebo poskytovateľ služieb vydá informácie týkajúce sa týchto služieb, ktoré sú v jeho držbe alebo pod jeho kontrolou, tomu, kto vydal príkaz podľa odseku 1.
Section 115 of the Code of Criminal Procedure	**§ 115 Trestného poriadku**
(8) If the interception and recording of telecommunication operations did not find any facts relevant to the criminal proceedings, the law enforcement authority or the competent department of the Police Force must destroy such recordings in the prescribed manner without undue delay. A transcript on the destruction of the recordings shall be entered into the file. The authority, by whose decision the matter was finally concluded and, in proceedings before the court, the presiding judge of the court of first instance, shall notify the	(8) Ak sa pri odpočúvaní a zázname telekomunikačnej prevádzky nezistili skutočnosti významné pre trestné konanie, orgán činný v trestnom konaní alebo príslušný útvar Policajného zboru musí získaný záznam predpísaným spôsobom bez meškania zničiť. Zápisnica o zničení záznamu sa založí do spisu. O zničení záznamu osobu uvedenú v odseku 3, ktorá nemá možnosť nazerať do spisu podľa tohto zákona, upovedomí orgán, ktorého rozhodnutím sa vec právoplatne skončila, a v konaní pred súdom predseda

person referred to in Subsection 3, who does not have the possibility of inspecting the file under this Act, on the destruction of the recordings within three years after the final termination of the criminal prosecution in the given matter; this shall not apply if it is performed on a particularly serious crime or a crime committed by an organised group, criminal group or a terrorist group, or if several persons participated in the commission of the criminal offence and, in relation to at least one of them, the criminal prosecution was not finally concluded, or if the provision of such information could obstruct the purpose of the criminal proceedings.	senátu súdu prvého stupňa do troch rokov od právoplatného skončenia trestného stíhania v danej veci; to neplatí, ak sa koná o obzvlášť závažnom zločine alebo zločine spáchanom organizovanou skupinou, zločineckou skupinou alebo teroristickou skupinou, alebo ak sa na trestnom čine podieľalo viac osôb a vo vzťahu aspoň k jednému z nich nebolo trestné stíhanie právoplatne skončené, alebo ak by poskytnutím takej informácie mohol byť zmarený účel trestného konania.
(9) The provisions of subsection 1 through 8 shall apply accordingly to content data or traffic data that is transmitted through a computer system in real time.	(9) Ustanovenia odsekov 1 až 8 sa primerane vzťahujú na obsahové údaje alebo prevádzkové údaje, ktoré sú v reálnom čase prenášané prostredníctvom počítačového systému.
Section 116 of the Code of Criminal Procedure	**§ 116 Trestného poriadku**
(1) In criminal proceedings for an intentional criminal offence, an order for the determination and notification of data on the performed telecommunications operation, which is subject to telecommunications privacy, or subject to personal data protection, which is necessary to clarify the facts relevant to the criminal proceedings, may be issued.	(1) V trestnom konaní pre úmyselný trestný čin možno vydať príkaz na zistenie a oznámenie údajov o uskutočnenej telekomunikačnej prevádzke, ktoré sú predmetom telekomunikačného tajomstva alebo na ktoré sa vzťahuje ochrana osobných údajov, ktoré sú potrebné na objasnenie skutočností dôležitých pre trestné konanie.
(2) The warrant for the establishment and notification of data on the performed telecommunication operations shall be issued by the presiding judge, before the commencement of the criminal prosecution or in the preliminary hearing upon the petition of the public prosecutor, the judge for preliminary hearing, in writing which must be justified by its merits; the warrant shall be served to the persons referred to in Subsection 3.	(2) Príkaz na zistenie a oznámenie údajov o uskutočnenej telekomunikačnej prevádzke vydáva písomne predseda senátu, pred začatím trestného stíhania alebo v prípravnom konaní sudca pre prípravné konanie na návrh prokurátora, ktorý musí byť odôvodnený aj skutkovými okolnosťami; príkaz sa doručí osobám uvedeným v odseku 3.
(3) The legal entities or natural persons that provide the telecommunication operations must notify the presiding judge and, in the preliminary hearing, the public prosecutor or police officer, about the data on the performed telecommunication operations.	(3) Právnické osoby alebo fyzické osoby, ktoré zabezpečujú telekomunikačnú prevádzku, oznámia predsedovi senátu a v prípravnom konaní prokurátorovi alebo policajtovi údaje o uskutočnenej telekomunikačnej prevádzke.
(4) The provisions of subsection 1 through 3 shall apply accordingly to content data or traffic data transmitted through a computer system.	(4) Ustanovenia odsekov 1 až 3 sa primerane vzťahujú na obsahové údaje alebo prevádzkové údaje prenášané prostredníctvom počítačového systému.

6.2.25 Slovenia

Provisions from Criminal Procedure Code

148th Article

(1) If there are grounds for suspicion that a crime was committed for which the offender is prosecuted ex officio, the police must take steps necessary to trace the offender, that the offender or participant does not hide or flee, to detect and protect the traces of a criminal offense and objects which may be used as evidence and to collect all information that could be useful for the successful conduct of criminal proceedings.

Article 149b

(1)If there are reasonable grounds for suspecting that a criminal offence for which a perpetrator is prosecuted ex officio has been committed, is being committed or is being prepared or organised, and information on communications using electronic communications networks needs to be obtained in order to uncover this criminal offence or the perpetrator thereof, the investigating judge may, at the request of the state prosecutor adducing reasonable grounds, order the operator of the electronic communications network to furnish him with information on the participants in and the circumstances and facts of electronic communications, such as: number or other form of identification of users of electronic communications services; the type, date, time and duration of the call or other form of electronic communications service; the quantity of data transmitted; and the place where the electronic communications service was performed.

(2) The request and order must be in written form and must contain information that allows the means of electronic communication to be identified, an adducement of reasonable grounds, the time period for which the information is required and other important circumstances that dictate use of the measure.

(3) If there are reasonable grounds for suspecting that a criminal offence for which a perpetrator is prosecuted ex officio has been committed or is being prepared, and information on the owner or user of a certain means of electronic communication whose details are not available in the relevant directory, as well as information on the time the means of communication was or is in use, needs to be obtained in order to uncover this criminal offence or the perpetrator thereof, the police may demand that the operator of the electronic

Article 164

(1) The police may even prior to the initiation seize items at 220th of this Act, if it would be dangerous to delay, and the conditions of the 218th of this Act to make home and personal investigation.

220th Article (seizure of items)

(1) Items which must be take under criminal or may be evidence in criminal proceedings shall be seized and deposited with the court or otherwise protect their storage.

(2) A person who has such items must delivered them at the request of the court. If he does not deliver the items, they can to be punished by a fine specified in the first paragraph of Article 78 of this Act, if he still don't want to do, he can be put in prison. Prison lasts until the surrender of items or until the end of criminal proceedings, but more than one month.

(4) Police officers may seize items mentioned in the first paragraph of this Article, when act in connection with 148 and 164 Article of this Act or when they issuing the court order.

Article 515

(3) If reciprocity or if so stipulated by an international treaty, international criminal-law also provides direct assistance to local and international bodies involved in the pre-trial and criminal proceedings. It may use modern technical means, in particular computer network devices for transmission of images, voice and electronic impulses.

6.2.26 Switzerland

Les bases juridiques régissant l'entraide judiciaire en matière pénale sont la *Loi sur l'entraide internationale en matière pénale* (EIMP), l'ordonnance y relative (OIEMP) et la *Convention européenne d'entraide judiciaire en matière pénale* (CEEJ). Ces textes règlent les principes généraux de l'entraide et la rendent subsidiaire à un cadre formel plus au moins strict. Citons par exemple l'art. 16 al. 2 CEEJ qui statue que les Parties peuvent décider dans quelle langue les demandes d'entraide doivent lui être adressées et que le principe de réciprocité est applicable. Etant donné que l'art. 28 al. 5 EIMP prévoit que les demandes d'entraide vers la Suisse doivent être rédigées en une langue nationale, les autres Etats peuvent exiger de même pour les demandes de la Suisse. Cela signifie que pour les demandes d'entraide envers les Etats dont la langue n'est pas maîtrisée par la Suisse, un service de traduction est indispensable.

Federal Act on International Mutual Assistance in Criminal Matters (Mutual Assistance Act, IMAC):
http://www.admin.ch/ch/e/rs/351_1/index.html

6.2.27 "The former Yugoslav Republic of Macedonia"

Chapter XXX of CPC, (Article 502-508)

Article 502
PROCEDURE FOR APPROVAL OF INTERNATIONAL JUDICIAL ASSISTANCE AND EXECUTION OF INTERNATIONAL TREATIES IN JUDICIAL CRIMINAL CASES

The international judicial criminal assistance will be performed according to the provisions of this law in line with the provisions of the European Convention for the international judicial assistance in the criminal matter with the Protocols, European Convection of United Nations for trans national organize crime and with other international treaties ratified in accordance with the Constitution of Republic of Macedonia

Article 503

(1) The applications of the domestic courts for judicial assistance in the criminal cases are delivered to the foreign agencies in a diplomatic course. In the same manner to the domestic courts are delivered the applications of the foreign agencies for judicial assistance, through the Ministry of Justice or directly from the competent court".(2) In emergencies, if there is mutuality, the applications for judicial assistance may be delivered by the Ministry of internal affairs.
(2) By law it will be determined which courts will be competent for giving international judicial criminal assistance and one court may be assigned to perform the work for all the courts on a certain region.

Article 504

(1) The Ministry of External Affairs will direct the application of the foreign agency for judicial assistance to the Ministry of Justice which will direct it for a procedure to the court on which region the person resides, who has to be handed a writ or who has to be examined or confronted or on which region another investigating act has to be conducted.
(2) In cases under Article 503, paragraph 2 of this Code, the Ministry of Internal Affairs directs the application to the court by the Ministry of Justice.
(3) On the permission and manner of the conducting of the act, which is the case in the application of the foreign agency, decides the court according to the domestic regulations.
(4) When the application refers to a crime for which according to the domestic regulations extradition is not allowed, the court will request an instruction from the Ministry of Justice.

Article 505

(1) The domestic courts may accept the application of the foreign agency with which it is requested execution of the criminal sentence by the foreign court or on the international court"
if it is determined with an international treaty, or if there is reciprocity or if the sanction is also pronounced by the domestic court according to the Criminal Code.
(2) The competent court reaches the verdict at the Chamber under Article 22, paragraph 6 of this Code. The public prosecutor and the counsel will be informed of the session of the Chamber.
(3) The local competence of the court is determined according to the last residence of the convicted person in the Republic of Macedonia- according to his place of birth. If the convicted person has not a residence nor was born in the Republic of Macedonia, the Supreme Court of the Republic of Macedonia will determine one of the courts to be competent before which the procedure will be conducted.
(4) The competent court is the court which is determined by law.
(5) In the pronouncement of the verdict under paragraph 2 of this Article, the court will insert the complete pronouncement and the title of the court with the foreign verdict and will pronounce a sanction, appropriate with the verdict pronounced by the foreign court". In the elaboration of the verdict will be presented the reasons for which the court has pronounced the sanction.

(6) Against the verdict may appeal the public prosecutor and the convicted person or his counsel.
(7) If the foreign citizen convicted by a domestic court or if the person authorised with an agreement submits an application to the first degree court the convicted person to serve the sentence in his country, the first degree court will act according to the international treaty
(8) Execution of the verdicts brought by the international court has to be performed in accordance with international treaties ratified in accordance with the Constitution of Republic of Macedonia.
(9) The Criminal Council from article 22 (6) of this law , on the local-govern first degree court, with verdict is confirming the authenticity and execution of the international court verdict and determines the manner of the sanction or the other measures of execution.

Article 505 –a

Domestic courts are proceeding upon the application of the foreign organs for overtaking the temporary measures for ensuring the article 203-a from this law, or towards the execution of measure for property confiscation and property interest and seizure of the objects towards which they have proceeded in accordance with the provisions from the international agreement.
The confiscated property and the property interest or the seized objects could be renounced with the court decision from the foreign country under certain conditions defined with the international agreement.
The domestic (national) courts under special defined conditions which are determined with the international contract can request determination of the temporary measures for ensuring that article 203- a of this law and execution of the confiscation of property and the property interest and seizing of the objects from the foreign organs
In the case when with the international agreement it is regulated that the confiscated property and the property interest shall be divided between the Republic of Macedonia and some other state, such of proposal will be delivered by the Ministry for justice. to the foreign country.

Article 506

For the crimes- making and releasing counterfeit bank notes, unauthorised production and trade with the narcotic drugs, psychotropic substances and precursors, trafficking with human beings, enterprising of pornographic material on child"
as well as other crimes in view of which with the international treaties it is determined centralisation of data, the court before which the criminal procedure is conducted, without delay, is obliged to deliver to the Ministry of Internal Affairs the data for the crime, the criminal and the legally valid verdict.

Article 507

(1) If on the territory of the Republic of Macedonia a crime has been committed by a foreigner who has a residence in a foreign country, out of the circumstances under Article 510 of this Code, to that country may be transferred all criminal records for the criminal prosecution and trial, if the foreign country is not against it.
(2) Before the decision for investigation is brought, the decision for transferring is brought by the competent public prosecutor. During the investigation, the decision on the proposal of the public prosecutor is brought by the investigating judge, and by the beginning of the trial, the Chamber (Article 22, paragraph 6).
(3) Transferring may be allowed for crimes for which a sentence to ten years is anticipated, as well as for the crimes- endangering the public traffic.
(4) If the damaged is a citizen of the Republic of Macedonia, transferring is not allowed if he resists it, unless it is allowed security for realisation of his lawful property request.
(5) If the accused is detained, from the foreign country it will be requested in the briefest possible way within 40 days to state whether it undertakes the prosecution.

Article 508

(1) The request by the foreign country in the Republic of Macedonia to be undertaken prosecution of a citizen of the Republic of Macedonia or of a person who has a residence in the Republic of Macedonia for a crime committed abroad, is directed with the records to the competent public prosecutor on whose region the person has his residence.
(2) If to the competent agency of the foreign country is submitted the lawful property request, it will be proceeded as if the request is submitted to the competent court.
(3) Of the refusal the criminal prosecution to be undertaken as well as whether the decision is legally valid, which has been brought in the criminal procedure, will be informed the foreign country which has submitted the request.

6.2.28 Turkey

(IV) THE RELEVANT TURKISH LEGISLATION ON JUDICIAL COOPERATION IN CRIMINAL MATTERS:

1. Constitution:
In the Constitution, there are two provisions related to judicial cooperation in criminal matters.
Article 90 regulates the relationship between the laws and international agreements inter alia on judicial cooperation in criminal matters.

Under Article 90, international agreements duly put into effect carry the force of law.
In accordance with Article 90, once an international agreement has been ratified, it becomes internal part of the national legal system and can directly be enforced.
No appeal to the Constitutional Court can be made with regard to these agreements on the ground that they are unconstitutional.
Article 38 of the Constitution provides that citizens shall not be extradited to a foreign country on account of an offence except under obligations resulting from being a party to the International Criminal Court.

2. Code and Laws:
There is no specific law on judicial cooperation in criminal matters but the following laws include some provisions on judicial cooperation in criminal matters:
a) Turkish Criminal Code (TCC), Law no: 5237, dated September 26, 2004, Article 18 governs extradition:
b) Law on the Organization and Functions of the Ministry of Justice (Law No. 2992):
Article 13/A of this Law provides that General Directorate for International Law and Foreign Relations is the central authority for execution of all kinds of judicial assistance requests in criminal matters.

3. International Agreements:
The main sources of international judicial cooperation in criminal matters in Turkey are the bilateral agreements between Turkey and other countries and the multilateral agreements to which Turkey is a party.
Multilateral Conventions of the Council of Europe and United Nations to which Turkey is a party.

Turkey is a party to "OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions" dated 21 November 1997. On the other hand Turkey is a member of "The Financial Action Task Force (FATF)" that is an inter-governmental body whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing.

If there is no bilateral and multilateral convention between Turkey and other country concerned, judicial cooperation in criminal matters is governed by international customs and principle of reciprocity.

4. Circulars
The subjects on the implementation of judicial cooperation in criminal matters are governed by the circulars issued by the General Directorate for the International Law and Foreign Relations of the Ministry of Justice.
As the recent TCC and TCPC came into force on 1 June 2005, a new circular no: 69 and dated 1/1/2006 has been issued. Mainly following issues are covered in this circular:
-Service of documents and letters rogatory including mutual legal assistance on the enforcement of the decisions on seizure and confiscation,
-Extradition, requests for search of offenders with Interpol Red Notice,
-Transfer of sentenced persons,
-Researches of addresses in abroad and provision of birth and death certificates and judicial records of foreign nationals.

(V) JUDICIAL COOPERATION IN PRACTICE

1. Mutual Legal Assistance

Turkey does not have any legislation that specifically deals with MLA. Bilateral and multilateral conventions are the main instruments in MLA practice in Turkey. The Ministry of Justice of Turkey plays a central role in judicial co-operation at large. General Directorate of International Law and Foreign Relations as a central authority receives the requests for mutual legal assistance and then transmits them to the competent authorities for execution. According to the general legal system, the competent authority may be either the court or the public prosecutor depending on the type of the assistance sought.

In cases of urgent requests under article 15 of the 1959 Convention (i.e. via Interpol), the Ministry of Interior will transmit the request to the Ministry of Justice for execution. Turkey has a positive approach to judicial co-operation, more precisely; incoming requests are carried out in a flexible and a cooperative manner. Turkey carries out requests of mutual assistance in criminal matters basically within the framework of "European Convention on Mutual Assistance in Criminal Matters."

6.2.29 Ukraine

Articles of CPC of Ukraine

CPC Article 159 Temporary access to objects or documents

1. Temporary access to the objects and documents means ability of the party of the criminal procedure on the will of the legal owner of some object or thing to operate with them, making copies and reading. Upon receiving warrant of investor-judge or judge – seize them.
2. Temporary access to the objects and documents can be carried out upon award of the investigator-judge or judge.

CPC Article 160 Petition on temporary access to objects and documents

1. Parties of the criminal procedure has a right to file a motion to investigator-judge or judge on the issue of temporary access to objects and documents, accept of the exclusions pointed in Article 161 of this Code. Investigator is empowered to file mentioned motion to investigator-judge that is approved by prosecutor.
2. Petition should contain:
- capsule review of the factual background of the criminal misdemeanor;
- legal qualification of the criminal misdemeanor according the Article in the Penal Code;
- objects and documents that are objectives of the temporary access procedure;
- grounds to believe that objects and things that need to be temporary accessed are owned by some person;
- objects and documents have a considerable value to identification of circumstances in criminal proceedings;
- ability to use information that can be received from objects and documents as evidence and impossibility to gain the given evidence in other way but by temporary access to objects and things;
- explanation of necessity to seize objects and things if the given issue is initiated by the party of criminal process.

CPC Article 161 Objects and things access to which is denied

1. Objects and things the access to which is denied:
- correspondence and other forms of data changing between attorney and his client or any other person that represents clients' law interests;
- objects attached to the given correspondence or other forms or data changing.

CPC Article 162 Objects and things that include secret data protected by law

Data that contains secret and stored in objects and documents is the following:
- information that belongs to mass media agencies or reporters that was given them on the basis of secrecy without uncovering source of its receiving;
- information that may contain doctor's secret;
- information that may contain notaries acts;
- confidential information including commercial data;
- information that can contain banking data;
- private correspondence of the person and other data of private character;
- information that is stored on the equipment of operators and telecommunication providers: connection, prescriber, the fact of access to the net, connection duration, content, routes of transmitting the data, etc;
- personal data that is stored in smb's private database or database that is possessed by the owner of the personal data;
- state secret.

CPC Article 163 Review of petition on temporary access to objects and things

1. Upon receiving petition on temporary access to objects and things investigator-judge or judge subpoenas holder (=owner) of objects and things that need to be temporary accessed accept of the case described by section 2 Article 163.
2. If the party of the criminal process that applied with petition proves sufficient grounds to regard the possible change or loss, or elimination of objects and documents, the mentioned petition can be reviewed by investigator-judge or judge without subpoena of the holder of objects and things.
3. Subpoena letter that is sent to the object/document owner contains provisions to retain data as it is from the time the letter was received.
4. Investigator-judge or judge that reviews petition on temporary access to objects and things in presence of the petition's initiator as well as holder of objects and documents. Scheduled review of the petition will be conducted not looking on the fact whether holder of objects and things is present or not.
5. Investigator-judge, judge serves warrant on temporary access to objects and things if it is proved that they:
- locate or can locate within the property of natural or legal person;
- bear distinctive meaning for identifying circumstances in criminal proceedings;
- does not include secret that is under protection of law.
6. Investigator-judge or judge also serves a warrant on giving permission for temporary access to objects and things when it is proven that the data stored on them might be used as evidence and that there is no other legal way to prove some circumstances of the criminal proceedings.
Access to law-protected information that is stored on objects and things is regulated by law. State secret data cannot be accessed by the person that has no right on it.
7. Investigator-judge, judge can also give an order to seize objects and things in case the party of the criminal process proves that there is a threat that they can be changed, deleted or lost.

Article 551 (Request for international assistance) says the following:

1. Judge, prosecutor or investigator with prior prosecutor's approval sends to the competent (central) body* of Ukraine request on international assistance within the scope of criminal proceeding that is being carried out.
2. Competent (central) body regards the received request in view of compliance to domestic laws and signed international treaties.
3. Upon positive decision competent (central) body sends a request to the competent body of requested Party within 10 days directly or through diplomatic channels.
4. Upon negative decision all the documents should be returned to the initiator within 10 days enlisting failings and mistakes.
* - General Prosecutor's Office

Article 552 Content and forms of request for mutual legal assistance

1. Content and forms of request for mutual legal assistance should correspond to the provisions of CPC of Ukraine or international treaty sighed by Ukraine. Request must be composed in the form of procuratory.
2. Request should contain:
- name of the requesting official body and competent body of requested Party;
- reference on international treaty for mutual legal assistance signed by Parties;
- name of criminal proceeding according to which the request is sent;
- capsule review of the criminal proceeding and its legal qualification;
- data about person, her full name, DOB, place of residence, citizenship, her procedural status and her liaison to the subject of criminal procedure;
- accurate list of needed procedural actions to be committed and their justification;
- persons that should be present during procedural actions and justification of this necessity;
- other information that can facilitate the obtaining of requested data.

3. Request must also contain a roster of Articles of domestic criminal legislation with the purpose to read rights and obligations of person who will interrogated as witness, expert, victim, suspect or accused. Request should also be accompanied with questions that must be put before mentioned persons.
4. Request on conducting searches, inspecting the crime scene, seize, arrest or confiscation of things should be carried out according to the requirements of this CPC.
5. It not compulsory to include into request data enlisted in sub-paras 4, 5, 8 of the para 2 of this Article.
6. While the request for mutual legal assistance is on pretrial stage, it should be approved by prosecutor who is in charge for controlling compliance with laws of pretrial investigation.

Article 557 of CPC Refusal on execution of request for mutual assistance

1. Requesting party may be refused in execution of request for mutual assistance in cases that are provided by international treaties that are signed by Ukraine.
2. While there are no international treaty with requesting Party, the initiator can be refused in execution of request for mutual assistance in the following cases:
- if the requests contradict Ukrainian Constitution and can harm sovereignty, security, public order, or other Ukrainian interests;
- if the requests refer to person who'd been already judged and court's decision came into effect;
- the requesting party does not support mutual law enforcement assistance when needed;
- request refers to the criminal misdemeanor that is not punishable due to the domestic laws;
- there are grounds to think that request is aimed to pursue persons because of their race, color of their skin, political, religious beliefs, sex, ethnic or social origin, property status, place of residence, or linguistic or other signs;
- request concerns the criminal misdemeanor or offense that is currently a subject of pretrial investigation or trial.

6.2.30 United Kingdom

Crime (International Co-operation) Act 2003.

Art. 7 Requests for assistance in obtaining evidence abroad

(1) If it appears to a judicial authority in the United Kingdom on an application made by a person mentioned in subsection (3)—

(a) that an offence has been committed or that there are reasonable grounds for suspecting that an offence has been committed, and

(b) that proceedings in respect of the offence have been instituted or that the offence is being investigated,

the judicial authority may request assistance under this section.

(2) The assistance that may be requested under this section is assistance in obtaining outside the United Kingdom any evidence specified in the request for use in the proceedings or investigation.

(3) The application may be made—

(a) in relation to England and Wales and Northern Ireland, by a prosecuting authority,

(b) in relation to Scotland, by the Lord Advocate or a procurator fiscal,

(c) where proceedings have been instituted, by the person charged in those proceedings.

(4) The judicial authorities are—

(a) in relation to England and Wales, any judge or justice of the peace,

(b) in relation to Scotland, any judge of the High Court or sheriff,

(c) in relation to Northern Ireland, any judge or resident magistrate.

(5) In relation to England and Wales or Northern Ireland, a designated prosecuting authority may itself request assistance under this section if—

(a) it appears to the authority that an offence has been committed or that there are reasonable grounds for suspecting that an offence has been committed, and

(b) the authority has instituted proceedings in respect of the offence in question or it is being investigated.

- "Designated" means designated by an order made by the Secretary of State.

(6) In relation to Scotland, the Lord Advocate or a procurator fiscal may himself request assistance under this section if it appears to him—

(a) that an offence has been committed or that there are reasonable grounds for suspecting that an offence has been committed, and

(b) that proceedings in respect of the offence have been instituted or that the offence is being investigated.

(7) If a request for assistance under this section is made in reliance on Article 2 of the 2001 Protocol (requests for information on banking transactions) in connection with the investigation of an offence, the request must state the grounds on which the person making the request considers the evidence specified in it to be relevant for the purposes of the investigation.

Art. 8 Sending requests for assistance

(1) A request for assistance under section 7 may be sent—

(a) to a court exercising jurisdiction in the place where the evidence is situated, or

(b) to any authority recognised by the government of the country in question as the appropriate authority for receiving requests of that kind.

(2) Alternatively, if it is a request by a judicial authority or a designated prosecuting authority it may be sent to the Secretary of State (in Scotland, the Lord Advocate) for forwarding to a court or authority mentioned in subsection (1).

(3) In cases of urgency, a request for assistance may be sent to—

(a) the International Criminal Police Organisation, or

(b) any body or person competent to receive it under any provisions adopted under the Treaty on European Union,

for forwarding to any court or authority mentioned in subsection (1).

Art. 13 Requests for assistance from overseas authorities

(1) Where a request for assistance in obtaining evidence in a part of the United Kingdom is received by the territorial authority for that part, the authority may—

(a) if the conditions in section 14 are met, arrange for the evidence to be obtained under section 15, or

(b) direct that a search warrant be applied for under or by virtue of section 16 or 17 or, in relation to evidence in Scotland, 18.

(2) The request for assistance may be made only by—

(a) a court exercising criminal jurisdiction, or a prosecuting authority, in a country outside the United Kingdom,

(b) any other authority in such a country which appears to the territorial authority to have the function of making such requests for assistance,

(c) any international authority mentioned in subsection (3).

(3) The international authorities are—

(a) the International Criminal Police Organisation,

(b) any other body or person competent to make a request of the kind to which this section applies under any provisions adopted under the Treaty on European Union.

Art. 14 Powers to arrange for evidence to be obtained

(1) The territorial authority may arrange for evidence to be obtained under section 15 if the request for assistance in obtaining the evidence is made in connection with—

(a) criminal proceedings or a criminal investigation, being carried on outside the United Kingdom,

(b) administrative proceedings, or an investigation into an act punishable in such proceedings, being carried on there,

(c) clemency proceedings, or proceedings on an appeal before a court against a decision in administrative proceedings, being carried on, or intended to be carried on, there.

(2) In a case within subsection (1)(a) or (b), the authority may arrange for the evidence to be so obtained only if the authority is satisfied—

(a) that an offence under the law of the country in question has been committed or that there are reasonable grounds for suspecting that such an offence has been committed, and

(b) that proceedings in respect of the offence have been instituted in that country or that an investigation into the offence is being carried on there.

An offence includes an act punishable in administrative proceedings.

(3) The territorial authority is to regard as conclusive a certificate as to the matters mentioned in subsection (2)(a) and (b) issued by any authority in the country in question which appears to him to be the appropriate authority to do so.

(4) If it appears to the territorial authority that the request for assistance relates to a fiscal offence in respect of which proceedings have not yet been instituted, the authority may not arrange for the evidence to be so obtained unless—

(a) the request is from a country which is a member of the Commonwealth or is made pursuant to a treaty to which the United Kingdom is a party, or

(b) the authority is satisfied that if the conduct constituting the offence were to occur in a part of the United Kingdom, it would constitute an offence in that part.

for forwarding to any court or authority mentioned in subsection (1).

Art. 19 Seized evidence

(1) Any evidence seized by a constable under or by virtue of section 16, 17 or 18 is to be sent to the court or authority which made the request for assistance or to the territorial authority for forwarding to that court or authority.

(2) So far as may be necessary in order to comply with the request for assistance—

(a) where the evidence consists of a document, the original or a copy is to be sent, and

(b) where the evidence consists of any other article, the article itself or a description, photograph or other representation of it is to be sent.

(3) This section does not apply to evidence seized under or by virtue of section 16(2)(b) or (4)(b) or 18(2)(b).

Art. 24 Evidence seized under the order

(1) Any evidence seized by or produced to the constable under section 22 is to be retained by him until he is given a notice under subsection (2) or authorised to release it under section 25.

(2) If—

(a) the overseas freezing order was accompanied by a request for the evidence to be sent to a court or authority mentioned in section 13(2), or

(b) the territorial authority subsequently receives such a request,

the territorial authority may by notice require the constable to send the evidence to the court or authority that made the request.

25 Release of evidence held under the order

(1) On an application made by a person mentioned below, the nominated court may authorise the release of any evidence retained by a constable under section 24 if, in its opinion—

(a) the condition in section 21(6) or (7) is met, or

(b) the overseas freezing order has ceased to have effect in the participating country.

(2) In relation to England and Wales and Northern Ireland, the persons are—

(a) the chief officer of police to whom a copy of the order was sent,

(b) the constable,

(c) any other person affected by the order.

(3) In relation to Scotland, the persons are—

(a) the procurator fiscal to whom a copy of the order was sent,

(b) any other person affected by the order.

(4) If the territorial authority decides not to give a notice under section 24(2) in respect of any evidence retained by a constable under that section, the authority must give the constable a notice authorising him to release the evidence.

6.2.31 United States

Title 18, U.S.C., Section 3512

(a) **Execution of Request for Assistance.—**
(1) **In general.—** Upon application, duly authorized by an appropriate official of the Department of Justice, of an attorney for the Government, a Federal judge may issue such orders as may be necessary to execute a request from a foreign authority for assistance in the investigation or prosecution of criminal offenses, or in proceedings related to the prosecution of criminal offenses, including proceedings regarding forfeiture, sentencing, and restitution.
(2) **Scope of orders.—** Any order issued by a Federal judge pursuant to paragraph (1) may include the issuance of—
(A) a search warrant, as provided under Rule 41 of the Federal Rules of Criminal Procedure;
(B) a warrant or order for contents of stored wire or electronic communications or for records related thereto, as provided under section 2703 of this title;
(C) an order for a pen register or trap and trace device as provided under section 3123 of this title; or
(D) an order requiring the appearance of a person for the purpose of providing testimony or a statement, or requiring the production of documents or other things, or both.

(b) **Appointment of Persons To Take Testimony or Statements.—**
(1) **In general.—** In response to an application for execution of a request from a foreign authority as described under subsection (a), a Federal judge may also issue an order appointing a person to direct the taking of testimony or statements or of the production of documents or other things, or both.
(2) **Authority of appointed person.—** Any person appointed under an order issued pursuant to paragraph (1) may—
(A) issue orders requiring the appearance of a person, or the production of documents or other things, or both;
(B) administer any necessary oath; and
(C) take testimony or statements and receive documents or other things.

(c) **Filing of Requests.—** Except as provided under subsection (d), an application for execution of a request from a foreign authority under this section may be filed—
(1) in the district in which a person who may be required to appear resides or is located or in which the documents or things to be produced are located;
(2) in cases in which the request seeks the appearance of persons or production of documents or things that may be located in multiple districts, in any one of the districts in which such a person, documents, or things may be located; or
(3) in any case, the district in which a related Federal criminal investigation or prosecution is being conducted, or in the District of Columbia.

(d) **Search Warrant Limitation.—** An application for execution of a request for a search warrant from a foreign authority under this section, other than an application for a warrant issued as provided under section 2703 of this title, shall be filed in the district in which the place or person to be searched is located.

(e) **Search Warrant Standard.—** A Federal judge may issue a search warrant under this section only if the foreign offense for which the evidence is sought involves conduct that, if committed in the United States, would be considered an offense punishable by imprisonment for more than one year under Federal or State law.

(f) **Service of Order or Warrant.—** Except as provided under subsection (d), an order or warrant issued pursuant to this section may be served or executed in any place in the United States.

(g) **Rule of Construction.—** Nothing in this section shall be construed to preclude any foreign authority or an interested person from obtaining assistance in a criminal investigation or prosecution pursuant to section 1782 of title 28, United States Code.

(h) **Definitions.—** As used in this section, the following definitions shall apply:

(1) **Federal judge.—** The terms "Federal judge" and "attorney for the Government" have the meaning given such terms for the purposes of the Federal Rules of Criminal Procedure.

(2) **Foreign authority.—** The term "foreign authority" means a foreign judicial authority, a foreign authority responsible for the investigation or prosecution of criminal offenses or for proceedings related to the prosecution of criminal offenses, or an authority designated as a competent authority or central authority for the purpose of making requests for assistance pursuant to an agreement or treaty with the United States regarding assistance in criminal matters.

6.3 Extracts of the Budapest Convention on Cybercrime

Article 31 – Mutual assistance regarding accessing of stored computer data

1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.

2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.

3 The request shall be responded to on an expedited basis where:

a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or

b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

Explanatory Report

Mutual assistance regarding accessing of stored computer data (Article 31)

292. Each Party must have the ability to, for the benefit of another Party, search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within its territory – just as under Article 19 (Search and seizure of stored computer data) it must have the ability to do so for domestic purposes. Paragraph 1 authorises a Party to request this type of mutual assistance, and paragraph 2 requires the requested Party to be able to provide it. Paragraph 2 also follows the principle that the terms and conditions for providing such co-operation should be those set forth in applicable treaties, arrangements and domestic laws governing mutual legal assistance in criminal matters. Under paragraph 3, such a request must be responded to on an expedited basis where (1) there are grounds to believe that relevant data is particularly vulnerable to loss or modification, or (2) otherwise where such treaties, arrangements or laws so provide.

Article 23 – General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Article 25 – General principles relating to mutual assistance

1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.

3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

Article 26 – Spontaneous information

1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.

2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

b The central authorities shall communicate directly with each other;

c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;

d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.

4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Article 28 – Confidentiality and limitation on use

1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:

a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or

b not used for investigations or proceedings other than those stated in the request.

3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.

4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

Article 35 – 24/7 Network

1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a the provision of technical advice;

b the preservation of data pursuant to Articles 29 and 30;

c the collection of evidence, the provision of legal information, and locating of suspects.

2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.