COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

www.coe.int/cybercrime

Strasbourg, version 20 May 2016 T-CY (2016)13

Cybercrime Convention Committee (T-CY)

Cloud Evidence Group

Emergency requests for the immediate disclosure of data

stored in another jurisdiction through mutual legal assistance channels or through direct requests to service providers

Compilation of replies to the questionnaire

Contents

Contact

Alexander Seger
Executive Secretary
Cybercrime Convention Committee (T-CY)
Directorate General of Human Rights and Rule of Law
Council of Europe, Strasbourg, France

Tel +33-3-9021-4506
Fax +33-3-9021-5650
Email: alexander.seger@coe.int

Background

The T-CY in December 2014 established the "Cloud Evidence Group" tasked to explore solutions on criminal justice access to evidence stored on servers in the cloud and in foreign jurisdictions, including through mutual legal assistance.

One of the options under review is procedures for emergency requests for the immediate disclosure of data stored in another jurisdiction through:

- mutual legal assistance channels, or
- direct requests to service providers

In this connection it is recalled that the establishment of emergency procedures had already been recommended in the T-CY Assessment report on mutual legal assistance adopted in December 2014:

> "Rec 8 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."

Parties and Observer States were, therefore, invited to reply to the below mentioned questions:

1. *Does your law allow a service provider operating in your territory to disclose data to domestic law enforcement in emergency situations without prior authorisation?*

   a. *What constitutes an emergency situation under your law?*
   b. *What category/ies of data (subscriber information, traffic data, content data) can law enforcement obtain in the case of an emergency situation?*

2. *Does your law allow a service provider operating in your territory to disclose data to foreign law enforcement in emergency situations without mutual legal assistance?*

   a. *What constitutes an emergency situation for these purposes?*
   b. *What category/ies of data (subscriber information, traffic data, content data) can foreign law enforcement obtain in the case of an emergency situation?*

3. *Do you have procedures for the expedited obtaining and disclosing of data to foreign authorities through mutual legal assistance channels in emergency situations?*

   a. *What constitutes an emergency situation for these purposes?*
   b. *What category/ies of data (subscriber information, traffic data, content data) can you disclose to foreign law enforcement in the case of an emergency situation?*
   c. *What are the procedures?*

4. *Any other comments*

Parties were asked to submit their replies by 15 April 2016.

The present document represents a compilation of the replies received.

REPLIES RECEIVED

PARTIES	**DATE**
Albania	
Armenia	
Australia	03 May 2016
Austria	31 Mars 2016
Azerbaijan	
Belgium	
Bosnia and Herzegovina	15 April 2016
Bulgaria	15 April 2016
Canada	
Croatia	8 April 2016
Cyprus	
Czech Republic	12 April 2016
Denmark	
Dominican Republic	24 April 2016
Estonia	
Finland	15 April 2016
France	18 April 2016
Georgia	
Germany	29 Mars 2016
Hungary	11 April 2016
Iceland	15 April 2016
Italy	15 April 2016
Japan	15 April 2016
Latvia	11 April 2016
Lichtenstein	
Lithuania	
Luxembourg	
Malta	
Mauritius	13 April 2016
Moldova	09 Mars 2016
Montenegro	11 April 2016
Netherlands	
Norway	18 May 2016
Panama	14 April 2016
Poland	
Portugal	18 April 2016
Romania	25 Mars 2016
Serbia	25 April 2016
Slovakia	14 April 2016
Slovenia	15 April 2016
Spain	15 April 2016
Sri Lanka	
Switzerland	22 April 2016
The former Yugoslav Republic of Macedonia	
Turkey	15 April 2016
Ukraine	
United Kingdom	
United States	15 Mars 2016
TOTAL	**29**

OBSERVERS	**DATE**
Andorra	
Argentina	
Chile	
Colombia	
Costa Rica	
Greece	
Ireland	
Israel	15 April 2016
Mexico	
Monaco	14 April 2016
Morocco	
Paraguay	
Peru	
Philippines	13 April 2016
Senegal	
South Africa	
Sweden	
Tonga	
TOTAL	**3**

AD HOC OBSERVERS	**DATE**
Belarus	14 April 2016
TOTAL	**1**

Compilation of replies

Q 1. Does your law allow a service provider operating in your territory to disclose data to domestic law enforcement in emergency situations without prior authorisation?

i. What constitutes an emergency situation under your law?
ii. What category/ies of data (subscriber information, traffic data, content data) can law enforcement obtain in the case of an emergency situation?

Austria	No
Australia	Yes. Sections 287 and 300 of the Telecommunications Act 1997 (Telecommunications Act) establish exceptions to the general prohibition established by the same Act, on the disclosure of any information or document that relates to contents or substance of a communication, or subscriber details, by a service provider. The exception allows for the disclosure of telecommunications data, including traffic data and subscriber information, in circumstances where there are reasonable grounds to believe that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of a person. 287 Threat to person's life or health Division 2 does not prohibit a disclosure or use by a person (the first person) of information or a document if: the information or document relates to the affairs or personal particulars (including any unlisted telephone number or any address) of another person; and the first person believes on reasonable grounds that the disclosure or use is reasonably necessary to prevent or lessen a serious and imminent threat to the life or health of a person. 300 Threat to person's life or health If information or a document is disclosed to a person (the first person) as permitted by section 287 or this section, the first person must not disclose or use the information or document unless: the disclosure or use is for the purpose of, or in connection with, preventing or lessening a serious and imminent threat to the life or health of another person; or the first person believes on reasonable grounds that the disclosure or use is reasonably necessary to prevent or lessen a serious and imminent threat to the life or health of another person. Telecommunications data may also be disclosed to advise individuals of an emergency or likely emergency under section 285A, 295V and 295W of the Telecommunications Act. However, in these situations, it is restricted to information in the integrated public number database. Moreover, the definition of 'emergency' (sections 275B, 275C, 275D of the Telecommunications Act and the Telecommunications (Data for emergency warning systems) Instrument 2010) is made with reference to Australian state and territory legislation and so in some cases is limited to emergencies affecting a particular Australian state or territory. Section 30 of the Telecommunications (Interception and Access) Act 1979 (TIA Act) establishes procedures for emergency requests authorising officers of a carrier to intercept telecommunications to disclose the location of a caller in situations where there is an honest belief that either another person (whether or not the caller) is dying, is being seriously injured or is seriously injured, or is likely to die or be seriously injured. Under this provision, only the location of the caller can be disclosed. 30 Emergency requests (1) Where:

	(a) a person is a party to a communication passing over a telecommunications system; (b) as a result of information conveyed by another party to the communication (in this section referred to as the **caller**) and of any other matters, the first-mentioned person forms the honest belief that either of the following emergencies exist: (i) another person (whether or not the caller) is dying, is being seriously injured or has been seriously injured; (ii) another person (whether or not the caller) is likely to die or be seriously injured; and I the first-mentioned person does not know the location of the caller; the first-mentioned person may: (d) in a case where the first-mentioned person: (i) is a member of a police force; and (ii) is of the opinion that tracing the location of the caller is likely to be of assistance in dealing with the emergency; request, or cause another member of a police force to request, an employee of a carrier to intercept, or to cause other employees of the carrier to intercept, the communication for the purposes of tracing the location of the caller; or I in a case where the first-mentioned person is not a member of a police force—inform, or cause another person to inform, a member of a police force of the matters referred to in paragraphs (a), (b) and (c). (2) Where a member of a police force is so informed, the member may, if the member is of the opinion that tracing the location of the caller is likely to be of assistance in dealing with the emergency, request an employee of a carrier to intercept, or to cause other employees of the carrier to intercept, the communication for the purposes of tracing the location of the caller. (3) Where, pursuant to a request made, or purporting to be made, by a member of a police force under subsection (1) or (2), an employee of a carrier intercepts a communication passing over a telecommunications system for the purpose of tracing the location of the caller, the employee shall: (a) communicate, or cause another employee of the carrier to communicate, the location of the caller to the person who made the request or to any other member of a police force; and (b) communicate particulars of the interception to the Managing Director of the carrier. (4) As soon as practicable after making to an employee of a carrier a request under, or purporting to be under, subsection (1) or (2), a member of a police force shall give, or cause another member of a police force to give, to the Managing Director of the carrier a written confirmation of the request that sets out the information given by the first-mentioned member to that employee in connection with the request.
Bosnia and Herzegovina	**Federal Ministry of Interior (F MoI):** No, it doesn't. Namely, under Article 86a of the Criminal Procedure Code of the Federation of Bosnia and Herzegovina (F BiH CPC), the service providers may submit such data only upon received Court Order. Article 86a of F BiH CPC provides possibility for police officers to submit a request to Court on needed provision of data, where the prosecutor only gives his/her approval and thus speeds up the procedure for acquisition and issuance of an Warrant pursuant to which a service provider (SP) submits the required data. **Brcko District (BD) Police:** As provided by both the Criminal Code and the Criminal Procedure Code of BD BiH, service providers submit such data on basis of previously acquired Warrant of Basic Court of Brcko District of Bosnia and Herzegovina issued upon the request of the Prosecutor's Office and the BD Police. **State Investigation and Protection Agency (SIPA)** provided a comment that they don't have a possibility to acquire the data directly from the service providers, and, consequently, are not in position to disclose such data to foreign law enforcement agencies. Acquisition of data from service providers and telecom operators is settled by Article 72.a of the BiH Criminal Procedure Code stating as follows: "The Court may order, upon proposition of Prosecutor or by him/her authorized official, to a telecom operator or another legal entity providing telecom services to submit the data on use of telecom services of the particular person, if

	such data may be used as the evidence in criminal procedure or benefit to gathering of information useful for the criminal procedure." The same CPC Article further settles in its paragraph (2) that the Prosecutor may order in emergency situations submission of described data, where the term of emergency was not precisely defined, but it depends of current situation, as well as the assessment and elaboration of the Prosecutor. **Ministry of Interior of Republic of Srpska (RS MoI)**: The Criminal Procedure Code of the Republic of Srpska (RS CPC) provides that Court may order upon a proposal of a Prosecutor or officials authorized by the Prosecutor to a telecom operator submission of the data relating to the use of telecom services. **F MoI:** Emergency is every situation in which a physical or legal entity necessitates urgent assistance of relevant services (e.g. firefighters, police, ambulance, as well as the other services for protection and rescue or relevant units of civil protection). **BD Police:** In context of cybercrime, emergency situation is <u>not</u> defined either by laws or bylaws of Brcko District of Bosnia and Herzegovina. **SIPA:** Term "emergency" is not precisely defined, but depends of the current situation, as well as the Prosecutor's assessment and elaboration. **RS MoI:** Pursuant to RS CPC, emergency situation is considered to be a situation constituting a risk of delay. **F MoI:** Urgent data acquired from ISP relate to subscriber information. **BD Police:** The answer is already provided. **RS MoI:** In emergent situations constituting a risk of delay, a prosecutor or by him/her authorized official may turn to Court with an oral request for issuance of Warrant and pursuant to this (oral) Court order acquire all the required data (subscriber information, traffic data, content data) from the telecom operator, provided that the operator possess such data.
Bulgaria	The Electronic Communications Act states that Bulgarian service providers may disclose data to Bulgarian law – enforcement agencies only after authorization from the court. The general provisions in this Act state that the data must be disclosed within 72 hours from the authorization by the court. The Minister of Interior or the Chairman of State Agency for National Security, or other authorized by them person, can determine specific deadline for producing the data. There is no definition in our law of emergency requests. In practice however, a request is considered as urgent if it is specified as such.
Croatia	The term "emergency situation", within the meaning set in the questionnaire, has no definition in the legislation of the Republic of Croatia. The provision that could possibly relate to the said term is the provision under the Croatian Criminal Procedure Act (*Zakon o kaznenom postupk*u) on the urgent collection of evidence, as follows (Article 212): "If there is danger arising from a delay, the police may conduct a search (Article 246), temporary seizure (Article 261), expert evaluation (Article 304), take fingerprints and prints of other body parts (Articles 211 and 307) even before the beginning of criminal proceedings for criminal offences punishable, under this Act, by imprisonment for up to five years". Aside from that, the practice is for each situation involving a specific request regarding computer data, due to the nature of such data, to be considered an emergency request.

	Data retention obligation is prescribed under the Electronic Communications Act (*Zakon o elektroničkim komunikacijama*); under Article 109 of the Act the operators of public communications networks and publicly available electronic communications services shall be obliged to retain electronic communications data referred to in Article 110 of this Act in order to make possible the conduct of the investigation, the discovery and the criminal prosecution of criminal offences, in accordance with a special law concerning criminal procedure and in order to protect defence and national security in accordance with special laws in the fields of defence and national security. Under Article 110 of the above Act, the data retention obligation includes the following type of data: data necessary to trace and identify the source of a communication; data necessary to identify the destination of a communication; data necessary to identify the date, time and duration of a communication; data necessary to identify the type of communication; data necessary to identify user communication equipment or what purports to be user equipment; data necessary to identify the location of mobile communication equipment.
Czech Republic	Yes. In case a service provider's assistance is needed, the procedure depends upon legal position of such a provider. In general, specified categories of data are always subject to an authorisation of a judge who issues a disclosure order. An authorisation (the disclosure order) is not required only in some cases of interception based upon an agreement of the intercepted person (see below the Section 88 Para. 5 of the Code of Criminal Procedure (CCP)): Interception and Recording of Telecommunications Section 88 (5) Without an order for interception and recording of telecommunication traffic may the authority involved in criminal proceedings order interception and recording of telecommunication traffic or perform it by itself, if the matter concerns criminal proceedings conducted for a criminal offence of trafficking in human beings (Section 168 of the Criminal Code), placing a child in custody of another person (Section 169 of the Criminal Code), illegal restraint (Section 171 of the Criminal Code), extortion (Section 175 of the Criminal Code), kidnapping of a child or a mentally challenged person (Section 200 of the Criminal Code), violence against a group of people and against an individual (Section 352 of the Criminal Code), dangerous threatening (Section 353 of the Criminal Code), or dangerous pursuit (Section 354 of the Criminal Code) provided that the user of the intercepted station consents with it. Neither the Czech Code of Criminal Procedure (CCP) nor the Act on Electronic Communications (Law No. 127/2005 Col.) specify "emergency situations" – in case such occur, promptness is a duty of the law enforcement authorities resulting from their position. In general such a constituting aspect is danger to life and health. Also, the following provisions are to be taken into account: Act No. 273/2008 Coll., on the Police of Czech Republic (the "Police Act") - the conditions stipulated in the Section 66(3) of the Police Act; - the Section 68 covering the search for persons and objects. Act No. 240/2000 Coll., on Crisis Management (the "Crisis Management Act") imposes further duties on legal entities and people conducting business in case of emergency. In particular, these subjects are obliged to cooperate upon request on the preparation of the emergency plan (i.e. a plan which includes a list of

	emergency measures and procedures for emergency situations) and fulfil the duties prescribed therein. Act No. 181/2014 Coll., on Cyber Security Cyber security event and cyber security incident § 7 (1) Cyber security event means an event which may cause security of information breach in information systems or security of services or security and integrity of electronic communication networks breach1. (2) Cyber security incident means information security breach in information systems or security of services breach or breach or integrity of electronic communication networks resulting from cyber security event. (3) Public authorities and natural and legal persons set out in § 3 c) to e) are obliged to detect cyber security events in their important network, critical information infrastructure information system, critical information infrastructure communication system or important information system. Under the Act on Cyber Security, the National Security Agency is entitled to issue decisions on reactive measures to address cyber security incidents or to secure information systems or networks and electronic communication services from cyber security incidents. The Act on Cyber Security provides the NSA with wide authority which may impose an obligation on ISP to shut down its network to the necessary extent. Act No. 127/2005 on Electronic Communications (Electronic Communications Act) Under the Sec. 97(3) of the Electronic Communications Act, a legal entity providing a public communications network or a publicly available electronic communications service (such as the ISP) is obliged to store traffic and location data for a period of 6 months and is obliged to disclose such data (including metadata) to the following authorities on request: the Police taking part in criminal proceedings, for the purposes and under the conditions prescribed by the Sec. 88a of the Criminal Procedure Code; the Police of the Czech Republic for the purposes listed in the Electronic Communications Act (such as preventing terrorism) and under the conditions prescribed by the Sec. 66(3) of the Act No. 273/2008 Coll., on the Police of the Czech Republic (the "Police Act"). The traffic and location data (including metadata) shall be provided to the authorities listed above in the manner described in particular by the Sec. 3 of the Decree No. 357/2012 Coll., on the preservation, transfer and deletion of traffic and location data. In relation to the form and extent of the data, the Sec. 97 of the Electronic Communications Act prescribes further conditions for the request of the traffic and location data, including the prior written approval of the Chairman of the Senate of the competent High Court. In case a provider is not subject to the Act on Electronic Communications (private mail servers, hostings), information like identity of an IP address user, registration data of an e-mail user, last connection, logs, shall be disclosed to the police without any authorisation.
Dominican Republic	No
Finland	The definition of "emergency situation" is not included in the legislation. Within the framework of this questionnaire this term might be interpreted so that it covers at least an imminent danger to life or health. Also the situations related to crime prevention have to be taken into account. Subscriber and contact information are available to everyone unless they are confidential based on the wish of the customer and the agreement between him/her and the service provider. Operators produce as commercial services public directories of subscriber and contact information related to the telecommunication connections.

	These services are open sources. According to Chapter 4, Section 3(2) of the Police Act in individual cases the police have the right to obtain from a telecommunications operator and a corporate or association subscriber on request contact information about a network address that is not listed in a public directory or data identifying a network address or terminal end device if the information is needed to carry out police duties. Similarly, the police have the right to obtain postal address information from organisations engaged in postal services. Provisions concerning messages (content data) and traffic data are in the Coercive Measures Act (806/2011; criminal investigation) and in the Police Act (872/2011; preventing an offence and averting an immediate danger to life or health). According to the Chapter 5, Sections 5 to 7 of the Police Act the police may be authorized by the court to target telecommunications interception at a network address or terminal end device in the possession of a person or presumed to be otherwise used by the person if on the basis of the person's statements, threats or behaviour there are reasonable grounds to believe that he or she would commit a serious offence mentioned in the Section 5. If it is likely that a message referred to in Section 5 and the related identification data can no longer be obtained through telecommunications interception, the police may be authorized by the court, in order to prevent an offence, to obtain data held by a telecommunications operator or a corporate or association subscriber subject to the preconditions laid down in Section 5. According to Chapter 5, Sections 8 and 10 of the Police Act police may use traffic data monitoring to prevent some offences, mainly serious ones. This requires an authorization by a court. If a matter concerning traffic data monitoring cannot be delayed, the decision on traffic data monitoring may be made by a police officer with the power of arrest until such time as the court has made a decision on the request for an authorization. The matter shall be brought for decision by a court as soon as possible, but no later than 24 hours after the action was started. Without the court decision police may use traffic data monitoring to avert an immediate danger to life or health. The Coercive Measures Act contains specific provisions on interception of telecommunications, as well as obtaining e.g. traffic data, location data and issuing data preservation orders. Those provisions are applied when investigating crime and also when executing such requests on mutual legal assistance, which require the use of coercive measures.
France	Le droit français comporte trois cadres d'enquêtes judiciaires : - la flagrance d'une durée pouvant aller jusqu'à 8 jours suite à la commission d'un fait délictuel ou criminel, permet aux forces de l'ordre de solliciter et obtenir un très grand nombre d'éléments, via des réquisitions judiciaires d'initiative (sans autorisation du magistrat). - l'enquête préliminaire dont les actes les plus attentatoires aux libertés individuelles doivent être autorisés par le procureur de la république - la commission rogatoire effectuée sous le contrôle d'un juge d'instruction D'autre part, d'une manière générale, l'article 223-6 du code pénal incrimine le fait pour quiconque de s'abstenir volontairement d'empêcher un crime ou un délit contre l'intégrité corporelle, ou de s'abstenir de porter assistance à une personne en péril. En rappelant les termes de cette disposition, les forces de l'ordre parviennent à obtenir dans ces cas d'urgence, des divulgations de données sans autorisation préalable. Dans les cadres d'urgence, toutes les données peuvent être obtenues.
Germany	In the German Criminal Procedure Code, an emergency situation is usually described

	with the term "exigent circumstances", which make a temporarily release of formal requirements (e.g. a court order or the order of the prosecutor's office) essential. There is no legal definition of "exigent circumstances", but according to judicature these circumstances are given, when complying with the formal requirements would mean that the purpose of the measure cannot be reached. In the Telecommunications Act this term is used as well to describe emergency situations (e.g. Section 113 subsection 2). Regulations in the Criminal Procedure Code Content and traffic data can in exigent circumstances be obtained by law enforcement authorities without a court order only by the order of the prosecutor's office (Section 100b Subsection 1 sentence 2, Section 101a Subsection 1 Sentence 1 German Criminal Procedure Code). If this order is not confirmed by the court within three working days, it will become ineffective. After the enactment of the law introducing a storage obligation and a maximum retention period for traffic data in December 2015 the conditions for collecting traffic data depend on the fact if the data asked for is stored for internal, enterprise related purposes (e.g. charging and billing) of service providers or if service providers only store the data because of the obligation to store it for a certain retention period. In the last case – storage because of the obligation and no storage for internal purposes – the law does not allow to collect the data without a court order, even if it's an emergency case and exigent circumstances are given (Section 101a subsection 1 Sentence 2 German Criminal Procedure Code). Subscriber information can be obtained without a court order (Section 100j German Criminal Procedure Code). Insofar a regulation of emergency cases is not necessary to enable law enforcement authorities to act immediately and ask for the data. Complementary Regulations in the Telecommunications Act/the Telecommunications Interception Ordinance For content data, in Section 12 of the Ordinance concerning the Technical and Organizational Implementation of Measures for the Interception of Telecommunications (Telecommunications Interception Ordinance – TKÜV)" of 3 November 2005 is laid down that the operator of a telecommunications facility must ensure that it can be notified by telephone at all times about the existence of a judicial order [meaning in this case: order of a court or a prosecutor's office] and the urgency of its implementation. The obligated party must ensure that it can receive a judicial order at any time within its usual business hours. Outside its usual business hours it must ensure receipt of the judicial order without delay, but at the latest six hours after notification. To the extent that a shorter time is stipulated in the judicial order, the steps necessary for this must be co-ordinated with the authorized body on a case-by-case basis. For the notification and the receipt of the judicial order, the obligated party must designate to the Federal Network Agency a place located in Germany that the authorised bodies must be able to contact at the cost of the usual fee for a simple telecommunications connection. According to Subsection 2 of Section 12 of the Ordinance, the obligated party must also introduce the steps needed to implement a judicial order on the basis of a copy of the judicial order transmitted to it in advance by a secure electronic path or by fax. An interception measure introduced on the basis of a fax must be switched off again by the obligated party if the original or a certified copy of the judicial order is not presented to it within one week after the transmission of the copy. For traffic data that is stored because of the obligation in Section 113b of the Telecommunications Act, according to Section 113c of the Telecommunications Act a service provider has to comply with a request, if it is submitted by the competent body and the regulation that allows the collecting of data is named.

	A request for subscriber information must in non-emergency cases be submitted to the service providers by the competent body in textual form with the regulation that allows the collecting of data explicitly named (section 113 subsection (2) sentence 1 of the Telecommunications Act). According to sentence (2) of section 113 subsection (2) the request can in exigent circumstances also be submitted formally different, e.g. verbally or by phone. In this case, the request has to be subsequently confirmed in textual form without undue delay, sentence (3) of section 113 subsection (2) of the Telecommunications Act. These regulations refer to criminal and non-criminal emergency requests equally.
Hungary	Based on specific agreements, cooperation service providers can give accelerated response to a request. In addition, some service providers (Vodafone, Hungarian Telekom) give LEAs direct access to their systems through secured channels. Thus, receiving an immediate response is ensured regardless of whether it is an emergency or not. To the best of my knowledge, transferring data on the basis of an emergency is not possible without a prior request. According to § 71 of the act on criminal proceedings the requesting authority shall give a period of time of at least 8 days within which deadline the organization contacted shall fulfil the request. Nevertheless, it is important to stress, that § 177 of the act on criminal proceedings provides for the possibility to forthwith implement the coercive measures defined by § 158 – i.e. ordering the reservation of data stored in IT systems – in urgent cases without a decision. In practice, in urgent cases the service providers give accelerated responses based on consultation, unless the official request arrives to them in a short time (via e-mail or fax) or eventually it is delivered to them personally. Experiences show that there are no difficulties in receiving accelerated response during working hours. Outside working hours and at the weekend solely the provisions of the specific cooperation agreements are to be followed. Through the HAR system of T-Mobile responses might be received within 10-15 minutes.
Iceland	(Preliminary response: There are no special provisions in law, but we are awaiting information on under which conditions service providers may have provided information to law enforcement on a voluntary basis and with reference to a general legal framework)
Israel	By section no. 4 to the Criminal Procedures (Powers of Enforcement – Communication Data) Law, 2007 The owner of "Bezeq license" – the internet service provider (provide IP address or provide infrastructure to connect to the web) can provide communication data as subscriber information, traffic data, content data – when asked by a police chief superintendent for a matter of emergency lifesaving or criminal act that dangerous the safety of others and need to dealing immediately. In a matter of other Internet service provider, which don't have a Bezeq license, because the law doesn't state anything about it there is a silent agreement that in case of life and death act the provider will deliver the data to the authorities.
Italy	Currently, the disclosure of information in the absence of an order issued by the judicial authority is not permitted. In special cases of emergency or when an immediate request to the judicial authority is not feasible, some data may be obtained, but the obligation of requesting an order as soon as possible remains. Currently there is no official definition of emergency situation, but generally, life-threatening circumstances are taken into account, as well as kidnappings and terrorist activities. Generally, and depending on the provider concerned, it is possible to obtain connection data (IP address), or those data provided by users when completing registration forms.
Japan	Regardless of the presence or absence of an emergency situation, it is possible for investigating authorities to obtain subscriber information, without a warrant from a

	judge, by making an inquiry on investigation related matters and to obtain contents data with a warrant from a judge or with service providers' lawful consent to provide them.
Latvia	According to "Electronic Communications Law" Section 19 (Duties of Electronic Communications Merchants) Electronic communications merchants have the following duties, to: (11) ensure in accordance with the procedures laid down in Section 71.1 of this Law the storage of data to be retained for 18 months, as well as the transfer thereof to pre-trial investigation institutions, bodies performing investigatory operations, State security institutions, the Office of the Public Prosecutor, the court if these institutions request such; (111) ensure the transfer of the traffic data to the institution referred to in Section 70 of this Law, if it requests the relevant data in the case and according to the procedures laid down in the law. Disclosure of data for the local law enforcement agencies can be realized in two ways- during operational activities (Operational activities Law) and during criminal investigation (Criminal Procedure Law). According to the "Operational activities Law" Section 9 Investigatory Inquiring- Investigatory acquisition of data from electronic information systems – that is, acquisition of such data, the storage of which is determined in the Law and which do not disclose the content of the information expressed or stored by a person – shall be performed with the permission of the head (chief) of the institution of the body performing investigatory operation or his or her authorised person, requesting data from natural persons or legal persons, which, using electronic information systems, process, store or transmit them. According to the "Criminal Procedure Law" Section 191 (Storage of Data located in an Electronic Information System) (1) A person directing the proceedings may assign, with a decision thereof, the owner, possessor or keeper of an electronic information system (that is, a natural or legal person who processes, stores or transmits data via electronic information systems, including a merchant of electronic communications) to immediately ensure the storage, in an unchanged state, of the totality of the specific data (the retention of which is not specified by law) necessary for the needs of criminal proceedings that is located in the possession thereof, and the inaccessibility of such data to other users of the system. (2) The duty to store data may be specified for a term of up to thirty days, but such term may be extended, if necessary, by an investigating judge by a term of up to thirty days. Section 192 (Disclosure of Data Stored in an Electronic Information System) (1) During the pre-trial criminal proceedings an investigator with the consent of a public prosecutor or a data subject and a public prosecutor with the consent of a higher-ranking prosecutor or a data subject may request, that the merchant of an electronic information system disclose and issue the data to be stored in the information system in accordance with the procedures laid down in the Electronic Communications Law. (2) During the pre-trial criminal proceedings the person directing the proceedings may request in writing, based on a decision of an investigating judge or with the consent of a data subject, that the owner, possessor or keeper of an electronic information system disclose and issue the data stored in accordance with the procedures provided for in Section 191 of this Law. (3) In adjudicating a criminal case, a judge or the court panel may request that a merchant of electronic communications discloses and issues the data to be stored in accordance with the procedures laid down in the Electronic Communications Law or that the owner, possessor or keeper of an electronic information system disclose and issue the data stored in accordance with the procedures provided for in Section 191 of this Law.

	According to the Cabinet regulation No. 820 "Procedures by which Pre-trial Investigative Institutions, Bodies Performing Investigatory Operations, State Security Institutions, Office of the Prosecutor and Court Request and a Merchant of Electronic Communications Transfers Data to be retained, and Procedures by which Statistical Information regarding Requests of Data to be Retained and Issuing thereof is Compiled" the matter of urgency is presumed to exist when. In those cases the information can be obtained within three hours, if the data requested have been retained within a time period of the last twenty-four hours or in one hour if requested the data concerning: the subscriber or registered user – initiator of the call – the given name, surname, personal identity number and address of a natural person or the name, registration number and address of a legal person; the International Mobile Subscriber Identity (IMSI) of the calling party; the International Mobile Equipment Identity (IMEI) of the calling party; if the user of a pre-paid service is anonymous – the date and time of the activation of the service and the location label (for example, Cell ID) from which the service was activated; the user ID(s) allocated; the subscriber or registered user to whom an Internet Protocol (IP) address was allocated at the time of the connection – the given name, surname, personal identity number of a natural person or the name, registration number and address, ID and telephone number of a legal person.
Mauritius	No, there must be an application made to the Judge in Chambers for an order. The section of the law does not speak of emergency situations but would be catered for if it is in the course of a criminal investigation. Section 12 of the Computer Misuse Cybercrime Act provides as follows:- 12. Disclosure of preserved data The investigatory authority may, for the purposes of a criminal investigation or the prosecution of an offence, apply to the Judge in Chambers for an order for the disclosure of— all preserved data, irrespective of whether one or more service providers were involved in the transmission of such data; (b) sufficient data to identify the service providers and the path through which the data was transmitted; or © electronic key enabling access to or the interpretation of data. An emergency situation could be one as governed under the Prevention of Terrorism Act, more specifically under section 25 of the said Act. The situation could be one which endangers national security. Section 3 of the Prevention of Terrorism Act provides illustrations of prohibited acts of terrorism. 25. Intelligence gathering Notwithstanding any other enactment, the Minister may, for the purposes of the prevention or detection of offences, or the prosecution of offenders, under this Act, give such directions as appear to him to be necessary to— communication service providers generally; (b) communication service providers of a specified description; I any particular communication service provider. (2) Before giving a direction under this section, the Minister may consult any communication service provider he deems fit to consult. (3) A direction under this section shall specify the maximum period for which a communication service provider may be required to retain communications data. (4) In this section— "communication service provider" means a person who provides a postal, or an information and communication, including telecommunications, service; "data" means information recorded in a form in which it can be pro-cessed by equipment operating automatically in response to instructions given for that purpose.

	3. Prohibition of acts of terrorism Any person who— does, or threatens to do, or does an act preparatory to or in furtherance of, an act of terrorism; or (b) omits to do anything that is reasonably necessary to prevent an act of terrorism, shall commit an offence. (2) In this section, "act of terrorism" means an act which— (a) may seriously damage a country or an international organisation; and (b) is intended or can reasonably be regarded as having been intended to— seriously intimidate a population; (ii) unduly compel a Government or an international organisation to perform or abstain from performing any act; (iii) seriously destabilise or destroy the fundamental political, constitutional, economic or social structures of a country or an international organisation; or (iv) otherwise influence such Government, or international organisation; and I involves or causes, as the case may be— attacks upon a person's life which may cause death; (ii) attacks upon the physical integrity of a person; (iii) kidnapping of a person; (iv) extensive destruction to a Government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property, likely to endanger human life or result in major economic loss; (v) the seizure of an aircraft, a ship or other means of public or goods transport; (vi) the manufacture, possession, acquisition, transport, supply or use of weapons, explosives or of nuclear, biological or chemical weapons, as well as research into, and development of, biological and chemical weapons; (vii) the release of dangerous substance, or causing of fires, explosions or floods, the effect of which is to endanger human life; (d) interference with or disruption of the supply of water, power or any other fundamental natural resource, the effect of which is to endanger life. Data has the same meaning as provided in the Computer Misuse and Cybercrime Act
Moldova	No
Monaco	Oui. L'urgence est constituée dans les cas suivants : 1/ En cas de crime flagrant en application de : L'article 47 du code de procédure pénale : « Lorsqu'il y a crime ou délit flagrant ou dans les cas assimilés, ils (les officiers de police judiciaire) font tous actes nécessaires à l'instruction suivant les règles établies au titre VII du présent livre. Si le procureur général intervient, ils reçoivent ses instructions pour la suite de la procédure », et de l'Article 266 du code de procédure pénale : « Dans le cas de crime flagrant, les officiers de police judiciaire, auxiliaires du procureur général, sont tenus d'avertir immédiatement ce magistrat et le juge d'instruction. En attendant leur arrivée, ils prennent toutes mesures utiles afin d'éviter la disparition des preuves. Ils peuvent même, en cas d'extrême urgence, faire tous les actes de la compétence du procureur général, dans les formes et suivant les règles ci-dessus établies. Ils transmettent alors, sans délai, au procureur général les procès-verbaux, les objets saisis et tous les renseignements recueillis, pour être procédé, sur ses réquisitions,

	comme il est dit au titre VI du présent code ». Parmi ces mesures d'instructions pouvant être ainsi mise en œuvre en urgence, figurent notamment celles prévues par l'article 106-1 du code de procédure pénale : « l'enregistrement et la transcription de correspondances émises par voie de télécommunications ou de communications électroniques, en cas de crime ou de délit passible d'une peine égale ou supérieure à un an. La décision d'interception est écrite. Elle n'a pas de caractère juridictionnel et n'est susceptible d'aucun recours. Les opérations prescrites en vertu du premier alinéa sont effectuées sous l'autorité et le contrôle du juge d'instruction ». 2/ lorsque le procureur général ou le juge d'instruction estiment que des mesures urgentes doivent être prises : En application : De l'article 87 du code de procédure pénale : « Le juge d'instruction prend toutes les mesures qu'il estime utiles à la manifestation de la vérité. Sauf en ce qui concerne l'interrogatoire de l'inculpé, il peut déléguer aux officiers de police judiciaire les actes d'information qu'il spécifie ». De l'Article 91 du code de procédure pénale : « À toute époque de l'information, le procureur général peut requérir du juge d'instruction tous actes lui paraissant utiles à la manifestation de la vérité et toutes mesures de sûreté nécessaires. Si le juge d'instruction ne suit pas les réquisitions du procureur général, il doit rendre une ordonnance motivée dans les cinq jours de ces réquisitions. Si le juge ne s'est pas prononcé dans ce délai, le procureur général peut, par simple requête, saisir la chambre du conseil de la cour d'appel qui statue au lieu et place du juge d'instruction et renvoie la procédure à celui-ci. La chambre du conseil peut également évoquer ». De l'article 111 du code de procédure pénale : « Si les circonstances l'exigent, le juge d'instruction peut ordonner qu'il sera procédé d'urgence à une expertise, sans en aviser les personnes indiquées à l'article 109. Les motifs d'urgence sont indiqués dans l'ordonnance, à peine de nullité des opérations ».
Montenegro	Our legislation stipulates that service providers who operate in our territory are allowed to provide data only pursuant to a previously issued order of the investigative judge, even in emergencies.
Norway	The Norwegian General Civil Criminal Penal Code has general provisions (Article 17 and 18) regarding exigent circumstances and self defense, and these provisions may be used also by law enforcement to get or give access to information. Based on current legal theory and practices, there must be an emergency situation a need to commit an act to save someone's person or property from an otherwise unavoidable danger, and this act would under normal circumstances not be legal the circumstances justifies regarding this danger as particularly significant in relation to the damage that might be cause by the act, and the act is proportional Generally, a running police investigation would not be sufficient to use these measures, but it could be sufficient if there's an urgent need to stop or prevent new crimes or to stop or prevent other significant risk for life and/or property. The crime(s) in question should not be too far ahead in time or too abstract in nature.

	The Criminal Procedure Act has several provisions regarding emergency situation. In several cases where court orders are needed, including legal access to communication data, production orders from prosecutors (Chief of Police) can be used, but the case must be presented to the court as soon as possible (within 24 hours for legal access to telecom networks). For the telecom sector, the Electronic Communications Act Article 2-9 regulates the duty of confidentiality for the providers regarding customer data and network data. The National Communications Authority (Nkom) may decide in cases where law enforcement asks for access to protected data, but in emergency situations, the provider may give the data directly to law enforcement without a prior authorisations from Nkom. Subscriber information are not considered protected by the duty of confidentiality. Neither is information on electronic communication address, including IP addresses and related subscriber information. In principle, all available data, within the purpose for the request and within proportion. As mentioned above, subscriber information from telecom companies, is not protected by the duty of confidentiality according to the Electronic Communications Act Section 2-9, third subsection. Data that could be access as a part of an emergency disclose, could include traffic data and PUK codes. One example: in a kidnapping case, the police in Asker and Bærum, Norway, got access from the mobile phone network provider to live mobile phone location data. This happened after the kidnapping victim had managed to call the police from a car booth.
Panama	No, Panamanian law does not allow said disclosure. Under these circumstances, there is no emergency situation under our laws (i.e., computer emergency) No category of data exists under our law to deal with emergency situations. Upon request and with the permission or authorization of the Supreme Court of Justice any kind of information may be obtained.
Philippines	No. Philippine domestic law does not require a local service provider to disclose data to domestic law enforcement agencies without prior authorization, even in emergency situations. It is only upon securing a court warrant that law enforcement authorities can issue an order requiring a service provider to disclose or submit a subscriber's information, traffic data or relevant data in its possession or control within seventy-two (72) hours from receipt of the order in relation to a valid complaint officially docketed and assigned for investigation and the disclosure is necessary and relevant for the purpose of investigation.
Portugal	According to the Portuguese law, obtaining content and traffic data within a criminal investigation always require an order from a judge (articles 187 and 189 of the Code of Pena Procedure and Article 18 of the Law on Cybercrime – Law nr 109/2009). On the other side, obtaining subscriber data, including the IP address used to establish a communication, requires an order from a prosecutor (Article 14, nr 1 and 4 of the Law on Cybercrime). It is not in place any emergency mechanism, in both cases (regarding subscriber information, traffic data and content). However, there is an exception: obtaining the so called "cellular localisation" (information respecting to the cellular tower used by a mobile telephone, when establishing a connexion to a GSM telephone network) is submitted to a particular regime. According to Article 252A of the Code of Penal Procedure, even a police

	officer can obtain information on "cellular localization" (Article 252A, nr 1) to, in case of danger to human life or of serious harm to physical integrity. This possibility can occur even if a formal investigation has not yet started Otherwise, data can be obtained via the expedited preservation of data (Article 12, Law on Cybercrime), combined with the expedited disclosure of traffic data (Article 13, Law on Cybercrime) and production order (Article 14, Law on Cybercrime) or search and seizure of computer data (Articles 15 and 16, Law on Cybercrime).
Romania	Under the national legislation data held by service providers can be disclosed to LEA or prosecutors only with prior authorization issued by a court, however a small range of data can be disclosed by service providers under a production order issued by the prosecutor e.g. billing information or data related to services offered by information society service providers (art. 170 para 2 the Code of criminal procedure) In both situations the orders are compelling the service provider to submit the data sought.
Serbia	According to the Law on Electronic Communications service provider is obliged to retain data on electronic communications. Access to retained data is not permitted without the consent of the user, except for a limited time and on the basis of a court order if it is necessary to conduct criminal proceedings or protect safety of the Republic of Serbia, in the manner provided by law. However, Criminal Procedure Code envisaged emergency situations in Article 158, providing that the public prosecutor or authorized police officers may, by exception, without a court order enter premises of the interest for pre-investigation or investigation purposes and without presence of witnesses undertake a search of the such premises or persons found there, and if needed, in accordance to Article 153, seize objects of the interest, including electronic data stipulated by Article 2 of CPC and Article 112 of the Criminal Code. Emergency situations for such procedure are: 1) with the consent of the holder of the premises; 2) if someone calls out for help; 3) in order to directly arrest the perpetrator of a criminal offence; 4) for the purpose of executing a court decision on the placement of a defendant in detention or on bringing him in; 5) for the purpose of eliminating a direct and serious threat to persons or property. If a search was undertaken after entering a premises, a record will be made of the entry into the premises and the search performed without a court order and presence of witnesses, in which will be specified the reasons for the entry and search.
Slovakia	With reference to a definition of an emergency situation under law of the Slovak Republic we would like to refer to the provisions of the Constitutional Act No. 227/2002 Coll. On national security in time of war, state of war, martial state and emergency state as amended, as well as the Act No. 387/2002 Coll. On State management in crisis situations outside war or a state of war as amended. Pursuant to Art. 1 par. 4 of the Constitutional Act a crisis situation shall mean a period during whom the security of a State is endangered or violated and constitutional bodies may after fulfilment of the conditions stipulated in this constitutional act declare for its solution a war, declare state of war or martial state or emergency state. The Act No. 387/2002 Coll. On State management in crisis situations outside war or a state of war further defines a crisis situation as a time period during whom security of a State is endangered or violated and constitutional bodies may after fulfilment of the conditions stipulated in the constitutional act or a special act declare for its solution martial state or emergency state or extraordinary situation.

	It has to be also noted that Code of Criminal Procedure (Act No. 301/2005 Coll. As amended) does not contain any specific provision defining *expresis verbis* which requests may be considered for emergency ones and when a situation may be considered for an emergency one. Act No. 351/2011 Coll. On Electronic Communications as amended specifies which data constitute the secrecy of electronic communication. Section 63 par. 1 provides that the subject of secrecy of telecommunication shall be: a) the contents of conveyed messages; b) related data of communicating parties (which are a telephone number, a business name and place of business of a legal person, or a business name and place of business of a natural person – undertaker or personal data of a natural person (which are a name and surname, title and permanent residence address; data published in the telephone directory shall not be subject to telecommunications secrecy). c) Traffic data (Traffic data shall mean any data related to the user and the particular conveyance of information in the network and arising during such a conveyance, which are processed for the purpose of conveyance of a communication in the network or for billing purposes) and d) Location data (Location data shall mean any data processed in a network or by a service that indicate the geographic location of the terminal of a user of a public service). Pursuant to Section 63 par. 6 of the Act No. 351/2011 Coll. A service provider may disclose only data subjected to the secrecy of telecommunications under par. 1 (letters b, c, d), and these shall be disclosed only on the basis of a written request and with the court's consent as stipulated in par. 7. In answering questions 1 and 2, it should be noted that a service provider cannot disclose data to domestic law enforcement authorities without prior authorization of the court (even in emergency situation). The same applies to disclosure of data to foreign law enforcement authorities. (see also reply to question no. 3).
Slovenia	According to the Electronic Communication Act, Article 104.a this is possible. In Article 104.a emergency situations are: Directly endangered life or body of the person To prevent dead or severe injury/body harm of the missing person To find a missing child According to the Article 104.a they can obtain: Traffic data Location data (last known geographical location, ID cell locations)
Spain	Spanish legislation does not expressly regulate the emergency situations and therefore, there is no special provision for data transfer to the law enforcement bodies in these cases, but the Code of Criminal Procedure generally regulates the transfer of certain data directly to the police without judicial authorisation. We can distinguish between the following types of data: Subscriber information: The Article 588.ter.m empowers the Public Prosecution and the Judicial Police to request the operators or service providers information relating to the ownership of a phone number or of any other communication means or, in the opposite sense, require the telephone number or the identifying data of any communication means; should this requirement not be met, the companies might incur the offence of disobedience. Existing data in the automated files of the service providers. Data not linked to a communication process. As provided for in Article 588.ter.j, unless required by a specific regulation, the Public Prosecution or the Police do not need, in principle, judicial authorisation to gather data kept by service providers or by people or entities who facilitate the communication when data kept are not linked to a communication process.

	Data linked to a communication process. Judicial authorisation shall be needed to gather these data, since the constitutional right to the privacy of communications can be affected. (Article 18 (3) of the Spanish Constitution). Information on contents. Judicial authorisation shall be always required for the transfer of contents.
Switzerland	Yes. Subscriber data and Traffic data can be disclosed without prior authorisation to domestic law enforcement authorities, not depending on the existence of an emergency situation. Content data, however, may be disclosed, without prior authorisation, but upon (also informal) request of a public prosecutor or a police officer, in emergency situations. Subsequently, an authorisation by the competent court has to be provided. According to Swiss law, situations of threat to life or physical condition are considered to be emergency situations, which may also include situations of missing persons.
Turkey	No. It is required to submit a prosecutor's order to obtain data in Turkey. However, if it is an emergency situation, the process can be accelerated.
USA	Yes, if the provider has a good faith basis to believe that there is an emergency. Emergency situation means a threat to life or of serious physical injury. All types of data can be disclosed.
Belarus	No

Q 2. Does your law allow a service provider operating in your territory to disclose data to foreign law enforcement in emergency situations without mutual legal assistance?

i. What constitutes an emergency situation for these purposes?
ii. What category/ies of data (subscriber information, traffic data, content data) can foreign law enforcement obtain in the case of an emergency situation?

Austria	No
Australia	There are no provisions in Australian law that allow for disclosure to foreign law enforcement in emergency situations.
Bosnia and Herzegovina	**F MoI:** No, it doesn't, but Bosnia and Herzegovina has a contact point available 24/7 to receive such requests. Upon request of the contact point, ISP "freezes" the required data that can be subsequently submitted to the Prosecutor once the Court Warrant is acquired. **BD Police**: Up to now, Brcko District Police did not have any requests or experience in the field, while the procedure for acquiring such data is elaborated under item 1. **RS MoI:** In accordance with the RS CPC, a telecom operator would provide such data to domestic or foreign law enforcement agencies solely upon a Court Warrant. **F MoI:** All the requests received through a 24/7 point of contact are considered as urgent. **BD Police:** In context of cybercrime, emergency situation is not defined either by laws or bylaws of Brcko District of Bosnia and Herzegovina. **RS MoI:** Pursuant to the RS CPC, emergency situation is considered to be a situation

	constituting a risk of delay. **F MoI:** Subscriber information. **BD Police:** As previously stated. **RS MoI:** Both foreign and domestic law enforcement agencies may receive such data under conditions prescribed by the law (same as under 1.a))
Bulgaria	The Electronic Communications Act states that Bulgarian service providers can disclose data to Bulgarian law-enforcement agencies. There are no regulations regarding providing data to foreign law-enforcement agencies.
Croatia	No
Czech Republic	No
Dominican Republic	No
Finland	See above the answer to question 1.b concerning public subscriber information and contact information. Public directories and other comparable sources of the service providers containing that kind of information are open sources and available also to foreign authorities regardless of the reason to get information. In other cases direct contacts between a domestic service provider and a foreign authority are not allowed. The ways of mutual legal assistance based on contacts between the law enforcement and judicial authorities have to be followed in the criminal investigation phase.
France	Non
Germany	No The manual information procedure according to section 113 of the Telecommunications Act allows service providers only to release subscriber information to the competent bodies named in section 113 subsection (3), which are national, domestic bodies. These bodies are - the (domestic) responsible authorities for the prosecution of criminal or administrative offences, - the (domestic) responsible authorities for averting danger to public safety or order and - the (domestic) federal and state authorities for the protection of the Constitution, the Federal Intelligence Service and the Federal Armed Forces Counter-Intelligence Office. It is statutorily regulated in section 113 subsection (2) sentence 1, that information is not allowed to be delivered to other public or non-public bodies. In practice, German service providers do not comply with requests of foreign authorities. In its latest transparency report the Deutsche Telekom AG clarified, that requests of foreign authorities are not answered due to the sole responsibility of the national authorities. According to the transparency reports of smaller service providers, foreign authorities did not submit any requests in the relevant period (2014).
Hungary	There are currently no such a legislation. Experiences show that national service providers do not reply directly to the requests initiated by foreign partner organizations.
Iceland	No
Israel	By section no. 4 to the Criminal Procedures (Powers of Enforcement – Communication Data) Law, 2007, An Israeli police officer action will be always needed. It's not possible to contact the foreign authority directly.
Italy	Laws currently into force in our country do not provide for direct contacts between Italian providers and foreign authorities. The information held by providers are protected by legal regulations (privacy act). Moreover, the disclosure of sensitive/personal data and/or confidential information without legal requirements or orders is not allowed.

	Any request for information shall be submitted through the usual legal assistance channels and, in case of urgent requests, it is possible to ask for the freezing of data by means of the designated point of contact in accordance with art. 35 of the Budapest Convention on Cybercrime. In case of emergency, foreign law enforcement agencies shall use the institutional communication channels for info about the data that may be obtained.
Japan	In Japan's criminal procedure code, there is no provision for a service provider to disclose data to foreign law enforcement in emergency situations and there is also no provision to prohibit a service provider from providing data to foreign law enforcement without following a procedure of mutual legal assistance. Regardless of the presence or absence of an emergency situation, it is possible for foreign law enforcement to obtain data from Japanese service providers without following mutual legal assistance procedure in a case where a service provider agrees to disclose data and the government of Japan has no objection to it.
Latvia	No special legal framework, which would determine the arrangements for cooperation between internet service provider and foreign law enforcement authorities without the Latvian Republic state authorities. This means that the disclosure of data for foreign law enforcement agencies takes place only in accordance with international agreements and mechanisms, including the letter of legal assistance and cybercrimes 24/7 contact point (24/7 Network).
Mauritius	No
Moldova	No
Monaco	Non.
Montenegro	No
Norway	Regarding mutual legal assistance, there are few few formal requirements regarding if a request from foreign law enforcement should be considered "mutual legal assistance. In principle, all data, within the principles described above.
Panama	Only through the corresponding channels established by mutual legal assistance treaties and by means of protocols can the Public Ministry, and not the service provider, provide the information needed to the foreign law enforcement agency in accordance with the law. Our law does not contemplate an emergency situation. No emergency situation exists under our law; therefore, it is necessary to comply with the protocols established by mutual legal assistance or other treaties.
Philippines	The Philippines adheres to the general principles relating to international cooperation. All relevant international instruments on international cooperation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purpose of investigations or proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in electronic form of a criminal offense, shall be given full force and effect. Since there is no domestic law specifically covering mutual legal assistance, the Philippines relies on treaty, convention or reciprocity as bases for mutual legal assistance. Unless there is mutual legal assistance between the Philippines and the foreign state and the request is coursed through the proper channels, a local service provider is under no compulsion or authority to disclose data to foreign law enforcement agencies, even in emergency situations.
Portugal	No. A Portuguese provider is only allowed to provide information within a MLA request. Nevertheless, according to Article 25 of the Law on Cybercrime, foreign criminal justice authorities can access data stored in a computer system located in Portugal,

	where publicly available, without prior request to the Portuguese authorities, if they respect the rules on transfer of personal data provided by the Portuguese law (which is on line with the European standards). Besides, also with respect of data protection rules, foreign criminal justice authorities can receive or access through a computer system located in its territory, data physically stored in Portugal, through legal and voluntary consent of the person legally authorized to disclose those data. In principle, a provider is not considered "the person legally authorized to disclose data".
Romania	No
Serbia	Law on Electronic Communications doesn`t provide possibility for service provider to disclose data to foreign law enforcement agencies without mutual legal assistance.
Slovakia	No
Slovenia	There are no special provisions in our national law about these issues. We have almost none experiences in this matter. Best practice for this matter would be international police cooperation via Interpol and/or Europol channels and 24/7 contact points.
Spain	As stated above, since there is no specific regulation on emergency situations, the way by which the foreign police may have access to data of a service provider operating within our territory would be through police cooperation or through the Public Prosecution Service. The requesting country's police should request the necessary data to the Spanish police or Public Prosecutor who would ask the service provider for such information, whenever the information requested is of the type they have direct access to, according to the classification made at the aforementioned point (subscriber data and data not linked to a communication process).
Switzerland	No. Mutual legal assistance channels or, where applicable, the usually faster track of police cooperation agreements have to be used. In the context of mutual legal assistance, the same procedures apply as with regard to domestic requests. Authorities seek to speed up procedures, where possible, for example by directly allowing the copying-in of ISPs based in our country when sending specific requests to Swiss authorities.
Turkey	No
USA	Yes, if the provider has a good faith basis to believe that there is an emergency. Emergency situation means a threat to life or of serious physical injury. All types of data can be disclosed.
Belarus	No

Q 3. Do you have procedures for the expedited obtaining and disclosing of data to foreign authorities through mutual legal assistance channels in emergency situations?

i. **What constitutes an emergency situation for these purposes?**
ii. **What category/ies of data (subscriber information, traffic data, content data) can you disclose to foreign law enforcement in the case of an emergency situation?**
iii. **What are the procedures?**

Austria	No
Australia	The *Mutual Assistance in Criminal Matters Act 1987* (Commonwealth of Australia) does not include specific provisions for emergency assistance. Requests made through mutual legal assistance channels are assessed by the Australian Central

	Authority and prioritised as appropriate, including where the requesting foreign authority asks that requests be expedited in emergency situations. The Australian Central Authority can receive and action requests made in electronic form provided those requests include sufficient information to provide the requested assistance. The types of data that can be provided and the timeframe in which mutual legal assistance requests can be responded to depends upon a number of factors including Australia's domestic legislation and the capacity of law enforcement agencies to action requests (for example, obtain and execute search warrants).
Bosnia and Herzegovina	**F MoI:** No, we don't. Bosnia and Herzegovina has a 24/7 point of contact to receive such urgent requests. **BD Police:** The answer is already stated. **Directorate for Coordination of Police Bodies of Bosnia and Herzegovina (Directorate)**: By being Bosnia and Herzegovina's the 24/7 point of contact for provision of assistance to local and foreign authorities in the procedures relating to cybercrime and provision of data pursuant to Article 35 of the Convention, the BiH Directorate for Coordination of Police Bodies had one person working in the NCB Unit of Sector for Operative Police Cooperation to undertake such activities as of the end of 2011. In accordance with above mentioned Article 35 of the Convention, the 24/7 point of contact in each participating country needs to be constantly available for provision of technical advice and arrangement of protection of electronic data required by a foreign 24/7 point of contact. In accordance with Article 25 (1) of the Convention, the countries provide each other with mutual assistance in the widest scope possible to enable investigations or procedures on crimes relating to computer systems and data or to gather evidence on a cybercrime. Up to now, we have received a number of requests of local police bodes in a manner provided by Articles 29 and 30 of the Convention. **RS MoI:** The procedure for cooperation with foreign agencies is settled by the Law on International Legal Assistance in Criminal Matters and cover both regular and emergent cases. The cooperation is also conducted through INTERPOL. **F MoI:** All of the requests submitted through the 24/7 point of contact are considered as urgent and treated as such without delay. **BD Police:** As previously stated. **RS MoI:** In the context of a request filed by a foreign authority, emergency situation is considered to be a situation constituting a risk of delay. **F MoI:** Subscriber information. **BD Police:** The answer is previously stated. **RS MoI:** Both foreign and local authorities may be provided with all categories of data under condition that all the requirements of the RS Criminal Procedure Code and Law on International Legal Assistance in Criminal Matters are met. **Directorate for Coordination of Police Bodies of Bosnia and Herzegovina**: Communication under the Convention is carried through an official e-mail of the contact point found in our institution. A received request is referred to the e-mail address of the contact point responsible for cybercrime in a foreign signatory to the Convention for the purpose of its further proceedings. The requests usually require urgent "freezing" of the data found on the foreign servers with an aim to secure the evidence in criminal proceeding from potential destruction or altering, while its submission would be subsequently required through diplomatic canals by a request for provision of international legal assistance. Up to now, the cooperation was established with competent authorities of USA, Croatia, Germany, the Netherlands, Island, and Switzerland.

	BD Police: The answer is already given. **RS MoI:** The procedure concerns a request submitted in accordance with the Law on International Legal Assistance in Criminal Matters.
Bulgaria	There is no definition in our law of emergency requests. In practice however, a request is considered as urgent if it is specified as such. Obtaining the data is again possible after court authorization.
Croatia	No
Czech Republic	The law does not provide for special procedures for expedited obtaining and disclosing of data to both Czech and foreign authorities, although, special attention is paid to priority MLA requests which may be sent also by electronic means. Sending MLA requests through other than usual channels is specified in the Section 8 of the Act on International Judicial Cooperation (Act No. 104/2013 Col.) which reads as follows: Section 8 Forms of Cooperation (5) If the matter clearly cannot be delayed and if there is no doubt about the credibility of the request, the judicial or central authority may initiate execution of actions of international judicial cooperation on the basis of a request of a foreign authority made via telephone, facsimile, electronically, through international police cooperation, personally via a representative of the foreign authority or otherwise. Unless an international treaty or this Act provide otherwise, they will always request the foreign authority to send the original of the request in documentary form within a time period specified by them.
Dominican Republic	No
Finland	In the case of criminal investigation confidential subscriber information, traffic data and content data can, in accordance with the legislation and international instruments on mutual legal assistance legislation, be disclosed to foreign law enforcement authorities regardless of the urgency of the situation. When executing such requests for mutual legal assistance, which require the use of coercive measures (to be defined in accordance with the Coercive Measures Act), conditions provided for in the Coercive Measures Act, are applied. This among other things means that the double criminality is required, which is applied in abstracto. There is however an exception to this rule, when a data preservation order is requested (section 15 of the Act on International Legal Assistance in Criminal Matters, 4/1994). Also in situations where the execution of the request does not require the use of coercive measures, the double criminality is not required when executing requests for mutual legal assistance. Measures in the case of criminal investigation are carried out through the channels of mutual legal assistance between the law enforcement and judicial authorities and following the Finnish legislation and applicable international instruments on mutual legal assistance. When dealing with emergency requests an effective 24/7 contact point and short response times are essential.
France	OUI – En cas d'urgence, conformément aux recommandations de l'article 25 §3 de la convention de Budapest, la France accepte l'utilisation des moyens de communication rapide, l'e-mail de préférence ou le fax (à tous les stades). Dans une hypothèse favorable, si les pièces d'exécution peuvent ensuite être acheminées également de façon dématérialisée, elles sont retransmises de cette façon.

	Une situation d'urgence est appréciée au cas par cas par l'autorité centrale et l'autorité judiciaire saisie, pas de définition stricte. Toutes catégories de données peuvent être obtenues. La procédure est celle de l'entraide judiciaire prévue par les conventions internationales en vigueur (échanges entre autorités judiciaires au sein de l'Union européenne et sinon, en fonction de la convention applicable entre autorités centrales ou par le biais de la voie diplomatique).
Germany	All measures available to the competent German authorities in equivalent domestic scenarios (s. question Nr. 1) can also be applied in execution of an MLA request from a foreign authority. This includes the specific procedures and competences foreseen in cases of exigent circumstances. Requests aiming only at subscriber data, can generally be handled even more expeditiously: The domestic procedural law (e.g. section 100 j of the Criminal Procedure Code, with the exception of the disclosure of access codes) does not stipulate any exclusive competence of the courts or prosecution services, which means, that subscriber data can also be obtained on police level. This allows foreign authorities to address these requests directly to the Federal Criminal Police (BKA) in its capacity as 24/7 contact point under various cooperation instruments. In executing the request the BKA can make use of the automated procedure foreseen in section 112 of the Telecommunication Act. This procedure enables the BKA to directly access certain kinds of subscriber data held by the most relevant providers, which further accelerates the execution of the request.
Hungary	Requests for data retention rapidly reach the Hungarian authorities through the systems of contact points operating 24/7 (CoE, G8). In addition, extraordinary requests may arrive through Europol and Interpol channels, the contact point of which are the National Police Headquarters National Criminal Cooperation Centre and the Riot Police's National Bureau of Investigation, Unit against Cybercrime acting as professional contact point. Experiences show that most of such requests are fulfilled by the Unit against Cybercrime of the Riot Police's National Bureau of Investigation. Upon the arrival of a request, it contacts as a matter of urgency the competent Public Prosecutor's Office, and based on the decision of the prosecutor it implements the necessary procedural actions before the arrival of the request for legal assistance.
Iceland	No
Israel	We are taking part in the 24/7 G8 system, and there are Unofficial police-police cooperation. In the case of a life and death situation there is a police national center that can immediately request the internet providers for information.
Italy	Currently, there are no expedited procedures to acquire data; however, it is possible to obtain the freezing of data regarding cybercrime. Foreign law enforcement agencies may obtain connection data (ip address), users registration forms, traffic data, mail boxes content and any other available data, whose conservation is allowed by law and possibly frozen in advance through appropriate orders of the judicial authority. Any request is subject to order issued by the competent judicial authority. Usual procedures consist in applying for mutual legal assistance, submitting requests through Interpol/Europol and all other institutional channels.
Japan	Although there are no special procedures asked in the question, there could be a case that Police, after considering a case of emergency situation individually and specifically, seeks to expedite a process within a framework of International Assistance in Investigation as necessary.

Latvia	-
Mauritius	No
Moldova	No
Monaco	La situation d'urgence n'est pas spécifiquement prévue par les dispositions internes applicables en matière d'entraide. L'urgence est signalée et motivée par les autorités étrangères dans leur demande. Les dispositions du code de procédure pénale citées au point suivant permettent d'obtenir tout type de données. d'entraide judiciaire internationale « le juge d'instruction peut déléguer tous les actes de l'information », et l'article 206 du code de procédure pénale dispose que « L'officier de police judiciaire commis exerce, dans les limites de la commission rogatoire, tous les pouvoirs du juge d'instruction ».
Montenegro	Yes, procedures provided for in Article 257a of the Criminal Procedure Code. A) Detecting the offender; collecting evidence to locate or identify a person and the search for a person on the run, B) Checking the identity, duration and frequency of communication with certain electronic communication addresses, identifying places where people performing electronic communication are located, as well as the identification marks of the device, the identification of the IMSI number; IMEI number and address of the internet protocol, IP address, or the person using that address. C) Procedure: e.g. a foreign law enforcement authority addresses us with the request via the contact person 24/7 in Montenegro (Budapest Convention), who will thereaater inform the acting prosecutor about this to obtain an order from the investigative judge for any of the actions provided for in Section B). The investigative judge issues the order within 4 hours, with the proviso that if a written order cannot be issued on time, these measures can be initiated on the basis of oral order of the investigative judge. However, the law enforcement authority must provide all the paperwork related to mutual legal assistance, which will be sent later, to substantiate and subsequently justify the issued order of the investigative judge.
Norway	In principle, all types of data, if necessary and proportional. There are no fixed procedures, apart from the general procedures regarding international law enforcement cooperation.
Panama	There are procedures in our legislation to obtain and provide information to foreign law enforcement agencies, based upon treaties and mutual legal assistance agreements; these procedures are not as expeditious and must fulfill all of the formalities demanded by procedural law. Emergency situations are neither contemplated nor described in our legislation. No categories exist, given that our legislation does not contemplate emergency situations. The procedures are based on mutual legal assistance agreements, on treaties or agreements to which Panama has adhered and on mutual reciprocity (all of these procedures must go through diplomatic channels.
Philippines	Yes. Under the Implementing Rules and Regulations of the Cybercrime Prevention Act of 2012, the Central Authority, i.e., the Department of Justice, Manila – Office of Cybercrime, shall accommodate a request from another State to search, access, seize, secure or disclose data stored by means of a computer system located within the country on an expedited basis where: 1) there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or 2) the instruments,

	arrangements and laws otherwise provide for expedited cooperation. Other procedures for the expedited obtaining and disclosing of data to foreign authorities through mutual legal assistance channels in emergency situations is provided for by treaty. For instance, under the Treaty on Mutual Legal Assistance in Criminal Matters Between the Republic of the Philippines and the United States of America, which was signed on 13 November 1994, a request for assistance is done in writing except that the Central Authority of the Requested State may accept a request in another form in emergency situations. In the latter case, the request shall be confirmed in writing within ten (10) days thereafter unless the Central Authority of the Requested State agrees otherwise. On the other hand, the Treaty Between Australia and the Republic of the Philippines on Mutual Assistance in Criminal Matters, which was entered into on 28 April 1988, provides that the request for assistance shall specify any time limit within which compliance with the request is desired. Also, a request to effect service of a document requiring the appearance of a person shall be made not less than 30 days before the date on which the personal appearance is required, unless the Requested State opts to waive such requirement in urgent cases. These treaties, however, do not define what an emergency situation is.
Portugal	No
Romania	The national legislation does not foresee with respect to disclosure of data any emergency procedure for domestic cases. Therefore, even if the case is related to an urgent mutual legal assistance request, the same provisions will be applicable. Nevertheless, in case of an emergency, the prosecutor, the judge and the service providers will treat the request with priority, meaning that information can be obtained in matters of hours or days, depending of the respective situation. In all cases the reply will be transmitted directly to the requesting authority, as well as with a copy to the central authority is required.
Serbia	Mutual legal assistance emergency request can be submitted directly to the 24/7 contact point in Special Prosecution for High-tech crime. Upon Prosecutor`s urgent request to the court, order for data preservation or disclosure will be issued and all necessary data could be disclosed by the service provider. According to Article 129 of the Law on Electronic Communications the obligation of the operator regarding data retention shall refer to the data necessary for: 1) tracing and identifying the source of a communication; 2) identifying the destination of a communication; 3) determining the beginning, duration and end of a communication; 4) identifying the type of communication; 5) identifying users' terminal equipment; 6) identifying the location of the users' mobile terminal equipment. Data revealing the content of a communication may not be retained, unless special evidentiary measures are not allowed.
Slovakia	Yes, because the expedited obtaining and disclosing of data to foreign authorities through mutual legal assistance channels in emergency situations is enabled -either under the principles and conditions stipulated in the relevant provisions of the Code of Criminal Procedure – CCP (Act No. 301/2005 Coll.), or -according to Articles 29 (Expedited preservation of stored computer data) and 35 (24/7 Network) of the Convention on Cybercrime, or -according to an international treaty (other than the Convention on Cybercrime) taking the precedence over the laws of the Slovak Republic (the so-called self-executing international treaties). It should be noted that a service provider cannot disclose data to foreign law enforcement authorities without prior authorization of the court (even in emergency situation or in case of emergency request).

	In general, the international judicial assistance in criminal matters is based on the principles and conditions stipulated in the Code of Criminal Procedure – CCP (Act No. 301/2005 Coll. as amended), that is ● a principle of reciprocity (pursuant to Section 479 of the CCP), or ● procedure according to foreign law (pursuant to Section 539 par. 2 of the CCP), or ● procedure according to an international treaty (other than the Convention on Cybercrime) taking the precedence over the laws of the Slovak Republic (the so-called self-executing international treaties pursuant to Art. 7 par. 5 of the Constitution). In case of emergency the international treaties enable to use the communication channels of the National Bureau of the INTERPOL (as 24/7 national point of contact in Slovakia) which closely cooperates with the Ministry of Justice of the Slovak Republic (mainly in the area of executing MLAs for the foreign judicial authorities), Office of the Prosecutor General of the Slovak Republic, Ministry of Foreign and European Affairs of the Slovak Republic, Corps of Prison and Court Guard and other competent national authorities. In this context, the execution of not only the MLAs, but also all emergency requests is ensured, in Slovakia, by the 24/7 alert duty of prosecutors and judges (within the district and regional prosecution offices and courts). The immediate executing of functions of prosecutors and judges outside the framework of the ordinary work regime is ensured by means of it (similarly, as for policemen within the 24/7 regime).
Slovenia	There are no special provisions/procedures about that matter. Best practice for this matter would be international police cooperation via Interpol and/or Europol channels and 24/7 contact points.
Spain	Neither the emergency situation nor the emergency process are specifically regulated, in general terms, in cases of international legal assistance, being applicable the criteria required for each case according to the country concerned, whether it is an EU State or a Third State. When the requesting country is signatory of the Budapest Convention, use is being made of the provision contained in Article 27 (9) of the Convention, which enables, in emergency cases, the communication and transmission of requests for legal assistance directly between judicial authorities, without prejudice of sending a copy to the central authorities. There is in Spain the network 24/7 of contact points set out in Article 35 of the Convention. Also the possibility provided for in Article 25 (3) of the Convention for emergency cases is being used, for which rapid means of communication as fax or e-mail are used in order to answer the requests for legal aid. Though no legal regulation is in place for emergency cases, it should be noted that in Conventions and Treaties signed by Spain, it is usual to include clauses stating that, in emergency cases, the request for legal assistance could be directly made between the authorities In cases of international legal assistance, the foreign authorities may request any type of data and, according to the nature of such information as afore mentioned, once the request for assistance has been received, information shall be gathered directly from service providers or it shall be either obtained by judicial authorisation.
Switzerland	Swiss domestic legislation on Mutual legal assistance contains a number of provisions regulating the issue of preliminary or temporary measures, trying to make sure that, in the context of a mutual legal assistance procedure, evidence is not lost and the best interests of parties affected can be protected. This possibility is not restricted to the issue of cybercrime or electronic evidence. Such measures may be implemented upon request of another State's authority or even before that, if such a request is foreseeable. An appeal against such a preliminary measure does not have a suspensive effect on the measure.
Turkey	No
USA	Yes, although the non-mutual legal assistance routes described above should be used

	first in emergencies. Emergency situation means a threat to life or of serious physical injury. All types of data can be disclosed. Procedure: Normal procedures apply, including satisfying the probable cause standard if content is sought. In an emergency, the US will work with the requesting State on an expedited basis so that, at the earliest possible moment, the required elements are written into the request in sufficient detail. It will speed the necessary legal papers so that courts may consider them more quickly. The US will then serve the legal papers on the provider upon receipt from the court, encourage the provider to produce the records urgently, and provide the records as quickly as possible to the requesting State. A very limited number of treaties permit a country to submit an oral request in urgent circumstances if it is confirmed in writing shortly thereafter
Belarus	No

iv. Any other comments

Austria	No
Australia	Police-to-police assistance Police-to-police assistance is available for the urgent disclosure of non-content data in line with the disclosure exceptions in the Telecommunications Act and the TIA Act. The Australian Federal Police Operations Coordination Centre (AOCC) Watchfloor are required to undertake emergency requests afterhours that are classified life-threatening. A life threatening communication is one which gives a person reasonable grounds to believe that there is a serious and imminent threat to the life or health of a person and may include events such as: a person being seriously injured or making threats of self-harm a bomb threat an extortion demand a kidnapping, or response to calls from vessels in distress. These requests are submitted in accordance with the Telecommunications Act and the TIA Act. Afterhours requests from foreign law enforcement agencies are directed through INTERPOL. When the official request has been received results will be disseminated back through INTERPOL. Any other urgent requests that do not fall within the above parameters are actioned accordingly during business hours. Telephone warrants in urgent circumstances Under the TIA, there are provisions allowing for warrant applications by telephone in urgent circumstances, for a Part 2-5 warrant (interception of telecommunications) or a stored communications warrant. These applications must be followed within one day by the provision of affidavits confirming the information provided in connection with the application. These provisions facilitate expeditious access to stored communications in urgent circumstances for domestic law enforcement, which reduces the time between domestic law enforcement agencies applying for said warrants and foreign law enforcement agencies receiving said information. 50 Issue of warrant on telephone application (1) As soon as practicable after completing and signing a warrant issued on a telephone application, a Judge or nominated AAT member shall: (b) inform the person who made the application on the agency's behalf of: (i) the terms of the warrant; and (ii) the day on which, and the time at which, the warrant was signed; and

	(c) give the warrant to that person. (2) A Judge or nominated AAT member who issues a warrant on a telephone application shall keep a copy of the warrant. 51 Action by agency after warrant issued on telephone application (1) A person (in this section called the applicant) who makes a telephone application on an agency's behalf shall comply with this section within one day after the day on which a warrant is issued on the application. (2) The applicant shall cause each person who gave information to the Judge or nominated AAT member in connection with the application to swear an affidavit setting out the information so given by the person. (3) The applicant shall give to the Judge or nominated AAT member: (a) the affidavit or affidavits; and (b) unless the applicant is the chief officer of the agency—a copy of an authorisation by the chief officer under subsection 40(3) that was in force in relation to the applicant when the application was made. 120 Stored communications warrants issued on telephone applications (1) An issuing authority who issues a stored communications warrant on a telephone application: (a) must, as soon as practicable after completing and signing the warrant: (i) inform the person who made the application, on behalf of the criminal law-enforcement agency concerned, of the terms of the warrant, the day on which it was signed and the time at which it was signed; and (ii) give the warrant to that person; and (b) must keep a copy of the warrant. (2) A person who makes a telephone application on a criminal law-enforcement agency's behalf must, within one day after the day on which a warrant is issued on the application: (a) cause each person who gave information to the issuing authority in connection with the application to swear an affidavit setting out the information so given by the person; and (b) give to the issuing authority: (i) the affidavit or affidavits; and (ii) unless the applicant is the chief officer of the criminal law-enforcement agency—a copy of an authorisation by the chief officer under subsection 111(3) that was in force in relation to the applicant when the application was made.
Bosnia and Herzegovina	**F MoI:** Federal Police Administration has no harmonised channels for mutual assistance in emergent reveal of the data kept by one authority to the other. The Federal Police Administration usually uses Interpol or the 24/7 point of contact to channel emergency communications with the other foreign police agencies. We do not have a practice of acquiring data and evidence by sending a direct police request to the internet service providers. In accordance with the Criminal Procedure Code of the Federation of Bosnia and Herzegovina, it is questionable if the evidence collected in such a way could be used in a criminal procedure conducted before a court. We believe that an establishment of channels and procedures to be used upon a request relating to life threatening emergency situations or other grave situations would considerably expedite the acquisition of data and evidences by resulting in improved work of police agencies. **The BiH Ministry of Justice (BiH MJ)** submitted its comment stating that there is no *lex specialis* settling this field. The Law on International and Legal Assistance does not specifically settle the international legal assistance on criminal matters, so we apply the Criminal Procedure Code. The Ministry provided the following comment: "A separate Section of the Criminal Procedure Code of Bosnia and Herzegovina (hereinafter: the BiH CPC) settles the term of *temporary seizure of objects and property,* and its provisions generally refer to cybercrime, too. Due to specificity of

	this type of crime, the BiH CPC's provisions regulate the means of conducting such activities and these would be separately enlisted. Pursuant to BiH Criminal Procedure Code, activities on collecting evidences and items to support evidencing in the criminal procedure as well as the activities to ensure evidences of importance for criminal procedure include, *inter alia*, the search of the apartment and other facilities and movable property pursuant to Article 51, where its paragraph (2) underlines the search of computers and devices for storing electronic data. This part of the Code also provides for the possibility of temporary seizure of objects and property. The search is grounded on a court warrant (Article 53) that has to be in written and elaborated. Principal determination of the court for the authority to decide on a search was set with an aim to protect the right to privacy and private life from unjustified and illegal undertakings over these fundamental rights of a person. This formal condition for performing a search is of general importance and applies to search of immovable/movable property and persons in both general and specific sense of the term. With respect to emergency cases mentioned in the Questionnaire, we would like to point out Article 56 of the BiH CPC. Pursuant to this provision, oral request for a search warrant may be submitted when there is a risk of delay. There must be a concrete risk of delay, which is evaluated on grounds of general and lifetime experience as well as of the conditions of the given case. The danger of delay needs to be restrictively interpreted and objectively assessed. Furthermore, it is provided that an oral request for a search warrant may be communicated through different means of electronic communication (telephone, fax, e-mail, radio, etc.). Temporary seizure of objects and property (Articles 65 through 74) is activity of collecting evidences for investigations, and in emergent cases it is possible to undertake it even before the initiation of the investigation (Article 66 relating to Article 218). Under Article 66, the objects that need to be seized or that could be used as evidence under the BiH Criminal Code may be temporarily confiscated without a court order provided there is a risk of delay. The condition for conducting a process activity relating to risk of delay must be such that the danger can be removed by this activity. In this sense, the risk of delay is considered as realistic if the relevant object could be destroyed, replaced or modified. Explicit legal provisions regulate that temporary seizure of objects and property may have the following forms: temporary seizure of objects to be confiscated under the BiH Criminal Code (Article 65 (1)); temporary seizure of objects that may serve as evidence in criminal procedure (Art. 65 (1)); collection of data kept on a computer or similar devices for automatic data processing (Art. 65 (6)); temporary seizure of letters, telegrams and other consignments (Art. 67); temporary seizure of documentation (Art. 68 (1)); provision of data relating to bank deposits and other financial transactions and business activities for certain persons (Art. 72 (1)); temporary suspension of certain financial transactions (Art. 72 (5)); and temporary seizure of property for the purpose of its preservation (Art. 73). Pursuant to the Criminal Code, seizure of objects is provided as a security measure for the objects that were used in a criminal act or were intended for a criminal act or are resulting from its undertake, and there is a risk of its reuse for conducting a criminal act so its seizure is considered as absolutely necessary to protect general security or moral reasons (Art. 74 of the BiH CC). The danger of the object(s) reuse in committing a criminal act, as well as the absolute necessity to protect general security or moral reasons is assessed in each individual case and is evaluated upon the specific circumstances of the criminal case. Legislation on temporary seizure of property also include the data saved in the computer or devices for automatic data processing, which enable permanent keeping of data and programs for the purpose of their subsequent use (Art. 65 (6)). It is considered that application of rules stemming from Article 65 (5) secures the proceeding guarantees relating to

	temporary seizure of computer and similar data. In the procedure of collecting the aforementioned data, one should pay a special attention to the regulations on confidentiality of collected data. In the context of questions on collecting evidence from telecommunication systems provided in the Questionnaire, it is very important to highlight the Code's Article 72a settling the procedures conducted by the court, prosecutor's office and authorised officials. For further clarity, here is the relevant Article: Article 72.a – Order to Telecommunication Operators If there are grounds for suspicion that a person had committed a criminal act, the Court may, upon a motion of Prosecutor or by him/her authorised official, order a telecommunication operator or another legal entity providing telecommunication services to submit the data on the use of telecommunication services of that particular person, if such data could be the evidence in the criminal proceeding or benefit to collection of information that may be used in the criminal proceeding. (2) In urgent cases, the Prosecutor may order the activities under paragraph (1) of this Article whereas the obtained data shall be sealed until issuance of a court order. The Prosecutor shall instantly inform on the conducted measures the judge who may issue an order within 72 hours. In case the judge for preliminary procedure does not issue the order, the Prosecutor shall return the data without opening it. (3) Activities from paragraph (1) of this Article may be also ordered for a person reasonably suspected for providing the perpetrator with the information or receiving the perpetrator's information related to criminal act or that the perpetrator uses his/her as mean of communication. (4) Telecommunication operators or the other legal entities providing telecommunication services shall facilitate the Prosecutor or the police bodies in conducting the measures under paragraph (1) of this Article." Out of the previously stated, one can conclude that temporary seizure of objects/property is a coercive measure in collecting evidence and items for the purpose of determination of facts in criminal procedure, its prevention, disabling its reuse or deprivation of someone else's property. Regardless of the wide scope of this process activity aimed at evidencing, the law had set the general rules of their application and prescribed the specificities of each enlisted form. The standards set in our national legislation are also applied in provision of international legal assistance.
Bulgaria	No
Croatia	No
Czech Republic	Providers are divided into two main groups within the Czech Republic. The first group provides connection to the internet. These are covered by the Electronic Communications Act. The second group provides a service on the internet except a connection to the internet. These are covered by the Act No. 480/2004 Coll., on Certain Information Society Services (which regulates, in accordance with the Community law, the liability and the rights and obligations of entities that provide information society services and disseminate commercial communications. It also defines terms for the proper interpretation and application of the Act). General view on obtaining data (off line data) by the law enforcement authorities: Disclosure of communication data Electronic Communications Act Under the Sec. 97(3) of the Electronic Communications Act – see the answer to the question 1.a. – the part titled Act No. 127/2005 on Electronic Communications (Electronic Communications Act). Criminal Procedure Code Under the Sec. 88a of the Criminal Procedure Code, the Police of the Czech Republic

	may only request traffic and location data on the basis of an order for the provision of such data. This order is issued by the competent Chairman of the Senate or a judge provided that the following conditions are met: a criminal proceeding is underway for one of the crimes listed in the Criminal Procedure Code; and this aim cannot be achieved by different means, or would be substantially more difficult to be achieved by different means. The above-mentioned order (which is a special type of a judicial decision) must be issued by: the Chairman of the Senate of the competent court; or the judge of the competent court within the preparatory proceedings, on the basis of a motion from the state prosecutor. The traffic and location data can be requested without such an order, provided that the user of the respective device consents to the provision of the data. The Government and law enforcement agencies in the Czech Republic do not appear to have any specific powers in order to compel the ISP to disclose the content of stored communications. Under the Sec. 97(5) of the Electronic Communications Act, a provider of a publicly-available telephone service is obliged to provide the Police of the Czech Republic on request with information from its database of participants, to the extent and in the form prescribed by the Information Decree. National security and emergency powers Electronic Communications Act Under the Sec. 99 of the Electronic Communications Act, a legal entity providing a public communications network or a publicly-available electronic communications service (such as the ISP) must provide priority access to the network for emergency communication participants (i.e. Ministries and other authorities) on the basis of a request from the Ministry of the Interior. The provider is entitled to restrict or interrupt the provision of publicly-available telephone services for this purpose. The provider is obliged to inform the Czech Telecommunication Office of the restriction or interruption. The restriction or interruption must not last any longer than necessary, and access to the emergency numbers must be maintained. Police Act Authorization of the Police of the Czech Republic Under the Sec. 39(11) of the Police Act, the police force has the right to interfere with the operation of electronic communication devices, the network and the provision of electronic communications services in the event of a threat to human lives, health or property with a value exceeding CZK 5 million. This typically includes situations where there is a threat of terrorism. The police is obliged to inform the Integrated Rescue System information point, the Czech Telecommunication Office, and to the necessary extent, the service provider (under the condition that informing the provider would not jeopardize the police force's fulfilment of its duties). Crisis Management Act The Crisis Management Act imposes further duties on legal entities and people conducting business in case of emergency. In particular, these subjects are obliged to cooperate upon request on the preparation of the emergency plan (i.e. a plan which includes a list of emergency measures and procedures for emergency situations) and fulfil the duties prescribed therein. Moreover, legal entities as well as people can also be required to perform duties above and beyond the duties prescribed by the emergency plan. The Crisis Management Act does not regulate any specific duties from communication service providers. A legal entity providing a public communications network or a publicly-available electronic communication service has a statutory obligation to provide the above-mentioned assistance. Theoretically, any provider's network could be shut down in responding to a crisis under the general principles of the Crisis Management Act but this is considered highly unlikely.

	Act on Cyber Security See the answer to the question 1.a. – the part titled Act No. 181/2014 Coll., on Cyber Security.
Dominican Republic	No
Finland	No
France	Non
Germany	No
Hungary	We welcome the possibility of direct communication in case of emergency. However, it is important that in the emergency procedure the service providers shall decide about the following question without the authorities' awareness: whether the person sending a request to the service provider is the representative of another state's authority, or a swindler, given the information provided it is a real emergency, thus providing the requested data without delay is in fact necessary. Therefore, such a recommendation would be necessary which handles the question of the appropriate verification of the requesting authority and harmonises the notion of emergency. This will make the recommendation compatible with the service providers' existing data protection obligation, and in this way the unreasonable refusal of requests can also be avoided.
Iceland	No
Israel	No
Italy	No
Japan	No
Latvia	No
Mauritius	No
Moldova	No
Monaco	Le projet de loi n° 934 relatif à la lutte contre la criminalité technologique, actuellement déposé devant le Conseil National monégasque (parlement) prévoit de compléter l'article 266 du code de procédure pénale en y visant de manière expresse les données informatiques. Par ailleurs un article 268-10 sera ajouté au code de procédure pénale détaillant les obligations incombant aux organismes publics et aux personnes morales de droit privé lorsqu'elles sont requises par les officiers de police judiciaire et établissant des sanctions pénales en cas de refus de répondre à ces réquisitions sans motif légitime :« Sur demande de 'officier de police judiciaire, qui peut intervenir par voie télématique ou informatique les organismes publics ou les personnes morales de droit privé mettent à sa disposition les informations utiles à la manifestation de la vérité, à l'exception de celles protégées par un secret prévu par la loi, contenues dans le ou les systèmes informatiques ou traitements d'informations nominatives qu'ils administrent. 37 L'officier de police judiciaire, intervenant sur réquisition du procureur général ou sur autorisation expresse du juge d'instruction, peut requérir des opérateurs et des prestataires de services chargés de l'exploitation des réseaux et des services de télécommunications et de communications électroniques de prendre, sans délai, toutes mesures propres à assurer la préservation, pour une durée ne pouvant excéder un an, du contenu des informations consultées par les personnes utilisatrices des services fournis par les opérateurs et prestataires. Les organismes ou personnes visés au présent article mettent à disposition les informations requises par voie télématique ou informatique dans les meilleurs délais. Le fait de refuser de répondre sans motif légitime à ces réquisitions est puni d'une peine d'un an d'emprisonnement et de l'amende prévue au chiffre 4 de l'article 26 du Code pénal. Les personnes morales peuvent être déclarées responsables pénalement, dans les conditions prévues par l'article 4-4 du Code pénal, de l'infraction prévue à l'alinéa précédent. La peine encourue par les personnes morales est l'amende suivant les modalités prévues par l'article 29-2 du Code pénal. Une ordonnance souveraine détermine les catégories d'organismes visés au premier

	alinéa ainsi que les modalités d'interrogation, de transmission et de traitement des informations requises. »
Montenegro	No
Norway	No
Panama	No
Philippines	No
Portugal	No
Romania	No
Serbia	No
Slovakia	The conditions for the use of the IT means without a prior consent of a person whose right to privacy has been interfered by the State authority using an IT mean result from the Act No. 166/2003 Coll. On the protection of privacy against unlawful use of IT means (Act on the Protection from the Interception). As regards the functioning of the prosecution service in time of war or state of war, Sections 44 par. 4 and 45 of the Act No. 153/2001 Coll. On the Prosecution as amended provides also for the organization of the prosecution in in time of war or state of war (the similar regime applies also in the judiciary according to the relevant provisions of the Act No. 757/2004 Coll. On the Courts and to amend and supplement certain acts).
Slovenia	No
Spain	Prior to the data transfer, other countries' law enforcement bodies may turn directly to Spain, through the Public Prosecutor of through the Police Forces, in order to preserve all sorts of data or contents whose transfer are to be later requested. The Article 588 octies of the Code of Criminal Procedure, in line with Article 16 of the Convention, regulates this assurance measure and empowers the Public Prosecutor and the Judicial Police to request data retention for a term of 90 days renewable up to 180 days. Even though data or content transfer processes for emergency cases are not yet regulated, it should be considered that the Law 25/2007 of 18 October, on the retention of data related to electronic communications and public communications networks is still in force after the sentence given by the Court of Justice of the European Union on the 8 of April of 2014, which establishes a term of 12 months to retain traffic data linked to a communication process. This guarantees that, in the event these data were requested they could be released –with previous judicial authorisation or even without it according to the above provisions- and within a short term, as the Article 7 of the Law establishes a maximum period of 7 calendar days for the transfer of data since the date the person required receives the request. In addition, every day of the year there are Judges and Prosecutors on-duty permanently in Spain, so in cases judicial authorisation is required such on-duty service ensures an immediate response to the data request submitted by the law enforcement authorities.
Switzerland	No
Turkey	No
USA	No
Belarus	The data which do not reveal information about the private life of citizens can be obtained by simple request signed by the investigator to the provider. This data includes information about the subscriber and the «static» traffic data (log-files, history etc.). This data LEA can obtain through NCP 24/7. At the same time, the data relating to the private life of citizens (the content of communications, talks, interception of traffic data in a real time, as well as statistics of telephone connections) can be obtained from the provider only an investigator's resolution authorized by the public prosecutor and registered in the prosecutor office.

	In this case we can obtain data only through mutual legal assistance channels. In the case of an emergency situation prosecutor or investigator can obtain data in a few days.

Appendix

www.coe.int/TCY

Strasbourg, 4 March 2016 T-CY(2016)10

Cloud Evidence Group and the T-CY Bureau

Questionnaire on "emergency procedures"

BACKGROUND:

The T-CY in December 2014 established the "Cloud Evidence Group" tasked to explore solutions on criminal justice access to evidence stored on servers in the cloud and in foreign jurisdictions, including through mutual legal assistance.

One of the options under review is procedures for emergency requests for the immediate disclosure of data stored in another jurisdiction through:

1. mutual legal assistance channels, or
2. direct requests to service providers

Information from Parties will furthermore allow for follow up to Recommendation 8 of the T-CY Assessment report on mutual legal assistance adopted in December 2014:

"Rec 8 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."

Parties and Observer States are invited to submit their responses in English or French in electronic form no later than 15 April 2016 to alexandru.frunza@coe.int.

Questionnaire on emergency requests

1. Does your law allow a service provider operating in your territory to disclose data to domestic law enforcement in emergency situations without prior authorisation?

    a. What constitutes an emergency situation under your law?
    b. What category/ies of data (subscriber information, traffic data, content data) can law enforcement obtain in the case of an emergency situation?

2. Does your law allow a service provider operating in your territory to disclose data to foreign law enforcement in emergency situations without mutual legal assistance?

    a. What constitutes an emergency situation for these purposes?
    b. What category/ies of data (subscriber information, traffic data, content data) can foreign law enforcement obtain in the case of an emergency situation?

3. Do you have procedures for the expedited obtaining and disclosing of data to foreign authorities through mutual legal assistance channels in emergency situations?

    a. What constitutes an emergency situation for these purposes?
    b. What category/ies of data (subscriber information, traffic data, content data) can you disclose to foreign law enforcement in the case of an emergency situation?
    c. What are the procedures?

4. Any other comments

Appendix 1: Background documents

T-CY(2015)10 Criminal justice access to data in the cloud: challenges
http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680304b59

T-CY(2016)7 Informal summary on issues and options under consideration by the Cloud Evidence Group
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016805a53c8

T-CY(2013)17rev assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime,
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c

T-CY (2014)16 Terms of reference of the Cloud Evidence Group,
http://www.coe.int/en/web/cybercrime/ceg

Conclusions of the Octopus conference 2015:
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680319026

Transborder Group: http://www.coe.int/en/web/cybercrime/tb