Electronic Evidence Country Fiche: PAKISTAN

1) DEFINITIONS

Pakistan
What are the definitions in your laws/regulations, if any, of:
Electronic evidence
In the legislation of Pakistan the term “electronic evidence” is not explicitly defined. However, the Prevention of Electronic Crimes Act, 2016 (PECA) Section 39(1)), refers to documents, elements, information “ for the collection of data in the electronic form” relating to an offence. According to Section 2 (f) of the Mutual Legal Assistance Act (Criminal Matters), 2020; Section 2 (g) of PECA and Section 2 of the Prevention of Electronic Crimes Ordinance, 2009 “electronic” means electrical, digital, magnetic, optical, biometric, electrochemical, electromechanical, wireless or electromagnetic technology; ...”. Under Section 2(s) the term “information” is defined, including text, messages, data, voice, databases, video, signals, software, computers, programmes, or any forms of intelligence as defined under the Pakistan Telecommunication (Re-organization) Act, 1996 (XVII of 1996) including object code and source code.
Computer system
According to the MLA Act 2020, Section 2(g) a “computer system” means any device or group of interconnected or related devices one or more of which, pursuant to a programme, performs automatic processing or recording data, and includes a mobile telephone and other telecommunication devices. Additionally, MLA Act 2020, Section 2(d) defines an “information system” as including an electronic system for creating, generating, sending, receiving, storing, reproducing, displaying, recording or processing any information.
Computer data
It seems that an explicit definition of computer data is not provided by Pakistan’s legislation. However, the source of electronic evidence is defined. It can be any electronic device, term defined under Section 2 (i) of the Preservation of Electronic Crimes Ordinance, 2009 as “electronic hardware which performs one or more specific functions and operates on any form or combination electrical energy”. According to Section 2 (e) of the PECA 2016 “device” includes: i. Physical device or article; ii. Any electronic or virtual tool that is not in physical form;

iii. A password, access code or similar data, in electronic or other form, by which the whole or any part of an information system is capable of being accessed; or
iv. Automated, self-executing, adaptive or autonomous device, programs or information system.
According to Section 2 (e) of the Prevention of Electronic Crimes Ordinance 2009, "data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in an electronic system including but not limited to computer program, text, images, sounds, video and information within a database or electronic system.

Categories of computer data (e.g. basic subscriber information, traffic data and content data)

Pakistani legislation provides definitions for specific types of data:

- "Subscriber information" Art 2, (v) of the Prevention of Electronic Crimes Ordinance, 2009 and PECA 2016, Art. 2 (zc) means any information in any form that is held by a service provider, relating to subscriber's services other than traffic data and by which can be established the type of communication service used, the technical provisions taken thereto and the period of service; the subscriber's identity, postal, geographic electronic mail address, telephone and other access number, billing and payment information, available on the basis of the service abatement or arrangement; or any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.
- "Traffic data" is provided by Section 2 (w) of the Prevention of Electronic Crimes Ordinance, 2009 and PECA 2016, Section 2 (zd) and refers to any data relating to a communication by means of an electronic system, generated by an electronic system that fanned a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.
- "Content data" means any representation of fact, information or concept for processing in an information system including source code or a program suitable to cause an information system lo perform a function Section 2(h) PECA 2016.

Finally, according to the MLA Act 2020, Section 2 (e) the general term "data" refers both to content data and traffic data.

Electronic surveillance or real-time collection of computer/communication data

The term "Electronic surveillance" appears not to be defined explicitly. However, Section 36 of PECA provides for procedure of "Real-time collection and recording of information".
Additionally, according to the IFTA (Investigation for Fair Trial Act, 2013) Chapter 1 on definitions (g) 'Intercepted material' means evidence collected under section 17 and will refer,-- (i) for the purposes of 'surveillance' to include, -- (a) data, information, or material in any documented form, whether written, through audio visual device, CCTV,

still photography, observation or any other mode of modern devices or techniques obtained under this Act; and (b) documents, papers, pamphlets, booklets; and
(ii) for the purposes of 'interception' to include e-mails, SMS, IPDR (internet protocol detail record or CDR (call detail record) and any form of computer based or cell phone based communication and voice analysis. It also includes any means of communication using wired or wireless or IP (internet protocol) based media or gadgetry.

Service provider (e.g. ISP, hosting)

Section 2, (u) of the Prevention of Electronic Crimes Ordinance, 2009 and PECA 2016, Section 2 (zb) "service provider" includes a person who:

i. Acts as a service provider in relate to sending, receiving, storing, processing or distributing of any electronic communication through an information system;
ii. Owns, possesses, operates, manages or controls a public switched network or provides telecommunication services; or
iii. Processes or store data on behalf of such electronic communication service or users of such service.

2) DATA RETENTION REGIME

Pakistan

Do you have any domestic laws that stipulate a mandatory retention period of electronic data? If so, for what types of data and for how long?

Based on Section 27 Retention of Traffic Data, Chapter IV (establishment of investigation and prosecution agencies), Preservation of Electronic Evidence Ordinance of 2009 a service provider shall, within its existing or required technical capability, retain its traffic data minimum for a period of ninety days (90) and provide that data to the investigating agency or the investigating officer when required.
Based on Chapter III, Section 29 Retention of Traffic Data, PECA, 2016 a service provider shall, within its existing or required technical capability, retain its specified traffic data for a minimum period of one year or such period as the Authority may notify from time to time and, subject to production of a warrant issued by the court, provide that data to the investigation agency or the authorized officer whenever so required.
For both the above provisions, the service providers shall retain the traffic data under sub-section (1) by fulfilling all the requirements of retention and its originally as provided under section 5 and 6 of the Electronic Transactions Ordinance, 2002 (LI of 2002).

The 2002 Electronic Transaction Ordinance (ETO) in points 5 and 6 imposes data retention requirements, establishing that under any law that certain document, record,

information, communication or transaction be retained shall be deemed satisfied by retaining it in electronic form if:

(a) the contents of the document, record, information, communication or transaction remain accessible so as to be usable for subsequent reference;

(b) the contents and form of the document, record, information, communication or transaction are as originally generated, sent or received, or can be demonstrated to represent accurately the contents and form in which it was originally generated, sent or received; and

(c) such document, record, information, communication or transaction, if any, as enables the identification of the origin and destination of document, record, information, communication or transaction and the date and time when it was generated, sent or received, is retained.

3) ADMISSIBILITY OF ELECTRONIC EVIDENCE IN THE CRIMINAL TRIAL

Pakistan
What is the requirement under your domestic law for electronic evidence to be admissible in criminal trial?
Under the mandates and prescriptions of section 3 of the Electronic Transactions Ordinance, 2002, it is emphasized that no document, record, information, communication or transaction shall be denied legal recognition, admissibility, effect, validity proof or enforceability on the ground that it is in electronic form and has not been attested by any witness. Section 164 of the Qanoon-e-Shahadat Order, 1984 (QSO) and section 27-B of the Anti- Terrorism Act 1997 (ATA) provide for the admissibility of e-evidence. It is essential that any e-evidence relied upon must be served on an accused in compliance with section 265-C of the Code of Criminal Procedure, 1898. Section 10 of the Mutual Legal Assistance Act of 2020, sets forth several limitations on the uses of evidence. It provides that any evidentiary material provided to a country by Pakistan as a result of a request for gathering of evidence under this Act, (a) shall not be used for any other purpose than the investigation, prosecution or judicial proceedings in respect of which the request for assistance was made; and (b) shall be inadmissible as evidence in any proceedings other than the proceedings for which it was obtained. Additionally, according to section 23 of the Act No. 1 of 2013 (Investigation for Fair Trial Act) the evidence including data, information, documents or any other material collected or received under the Act, shall be admissible as evidence in the legal proceedings

4) RECEIVING REQUESTS FOR ELECTRONIC EVIDENCE FROM OTHER STATES

4.1. **Direct requests** from foreign authorities to service providers

4.1.1. Requests for preservation

Pakistan
What legal framework(s) is/are applicable, if any?
It is not explicitly regulated by the law of Pakistan whether a request for preservation can be addressed directly to service providers within the country from foreign authorities.
Are the service providers in your country prohibited from or have limited capacity for executing such requests from foreign authorities?
Yes. All requests should go through the Ministry of Interior in Pakistan.
If they are prohibited or if there are limitations, are there any alternative options to preserve the data from your country, e.g. through police-to-police cooperation, specialized networks (e.g. G7/8 24/7 Network) or mutual legal assistance (MLA)?
The PECA 2016 is expedient to prevent unauthorized acts with respect to information systems and provide for related offences as well as mechanisms for their investigation, prosecution, trial and international cooperation with respect thereof and for matters connected therewith. Under this Act the procedure for preservation and acquisition of data is provided by Section 28 Chapter III. Further, according to Section 39 (2), PECA 2016 in the Pakistan Law there is the possibility, upon receipt of a request, of providing data directly to any foreign government, 24 x 7 network, any foreign agency or any international organization or agency for the purposes of investigations or proceedings concerning offences related to information systems, electronic communication or data or for the collection of evidence in electronic form relating to an offence or obtaining expeditious preservation and disclosure of data by means of an information system or real-time collection of data associated with specified communications or interception of data under this Act. Under Section 19 of the MLA Act of 2020 the procedure for the expedited preservation and disclosure of information systems is described. Upon request by a country setting forth: (a) the need for specified electronic data to be preserved; (b) the urgency of preserving it; (c) sufficient information to locate the electronic data; and (d) a statement that a request for production of the data will follow, the central authority may issue an order to any person in the Islamic Republic of Pakistan to preserve and safeguard such

data. The order under sub-section (1) shall lapse if the request for production is not received within forty-five (45) days of the request for preservation.

The Ministry of Interior has issued SOP (standard operating procedure) No. 8/3/2020-Law dated 8 April 2020 for Police-to-Police cooperation. Several channels are available for police-to-police cooperation and for the exchange of police information and intelligence, but certain channels appear most relevant:

- the national competent authorities (which are in some States referred to as designated single points of contact),
- the channel of regional/international organs (e.g. INTERPOL National Central Bureau or 24/7 Networks), and
- the liaison officer channel.

The legal competence to begin and direct criminal investigations belongs to the National Response Centre for Cyber Crimes (NR3C) of the Federal Investigation Agency.

A spontaneous information sharing is granted also under Art. 18 (4) and (5) of the United Nations Convention against Transnational Organized Crime, due to which the competent authorities of a State Party may, without prior request, transmit information relating to criminal matters to a competent authority in another State Party where they believe that such information could assist the authority in undertaking or successfully concluding inquiries and criminal proceedings.

Is a judicial order required from the requesting state?

No, there is no need of a judicial order from the requesting state.

Are there any time limits for data preservation? Any possibility of extension?

The procedure for preservation and acquisition of data is provided by Art. 28 Chapter III of the PECA 2016, which affirms that an authorized officer may, by written notice given to the person in control of the information system, require that person to provide that data or to ensure that the data specified in the notice be preserved and the integrity thereof is maintained for a period not exceeding ninety (90) days as specified in the notice. Provided that the authorized officer shall immediately but not later than twenty-four (24) hours bring to notice of the Court, the fact of acquisition of such data and the Court on receipt of such information may pass such orders as deemed appropriate in the circumstances of the case including issuance of warrants for retention of such data or otherwise.
The period for preservation of data may be extended by the Court if so deemed necessary upon receipt of an application from the authorized officer in this behalf.
This procedure is applicable in the context of international cooperation ex art. 39, upon receipt of a request.

Would service providers in your country notify the data subjects of the request?

No, the service provider will not notify the data subject to the request.

4.1.2. Requests for voluntary disclosure

Pakistan
What legal framework(s) is/are applicable, if any?
The law does not provide any applicable legal framework in this regard.
Are the service providers in your country prohibited from or have limited capacity for executing such requests from foreign authorities?
Yes, the Service Providers located in the territory of Pakistan do not have the capacity to execute requests from foreign authorities.
If they are prohibited or if there are limitations, are there any alternative options to preserve the data from your country, e.g. through police-to-police cooperation, specialized networks (e.g. G7/8 24/7 Network) or mutual legal assistance (MLA)?
In Pakistani law there is the possibility of providing data directly to other States. According to Art. 39 (2), PECA 2016 the Federal Government may forward to a foreign government, 24 X 7 network, any foreign agency or any international agency or organization any information obtained from its own investigations if it considers that the disclosure of such information might assist the other government, agency or organization etc., as the case be, in initiating or carrying out investigations or proceedings concerning any offence under this Act. The PECA 2016 provides general international cooperation measures, including broad provisions relating to spontaneous information, grounds for refusal, confidentiality and limitation of use and enabling powers to cooperate with respect to specialized investigative measures (Section 34). It is possible through police-to-police cooperation: INTERPOL National Central Bureau or 24/7 Networks. Additionally, under the 2009 Prevention of Electronic Crimes Ordinance Chapter IV Establishment of Investigation and Prosecution Agencies under Section 29 Pakistan provides regulations for trans-border investigative access. The Federal Government or the investigation agency may, without the permission of any foreign Government or international agency access publicly available electronic system or data notwithstanding the geographical location of such electronic system or data, or access or receive, through an electronic system, data located in foreign country or territory, if

it obtains the lawful and voluntary consent of the person who has the lawful authority to disclose it. Such access shall not be prohibited under the law of the foreign Government or the international agency. To be provided with further information, the investigating agency shall inform in writing to the Ministry of Foreign Affairs of Government of Pakistan Finally, spontaneous information sharing is always granted also under Art. 18 (4) and (5) of the United Nations Convention against Transnational Organized Crime.
Is a judicial order required from the requesting state? Are there any time limits?
No, there is no need of a judicial order from the requesting state.
Would service providers in your country notify the data subjects of the request?
No, the Service Providers do not notify the data subject of the request.
How can the process be simplified or quickened in emergency situations?
Information not provided.

4.2. Requests received by your central authority for **Mutual Legal Assistance (MLA)**

Pakistan
How do you execute MLA requests for electronic evidence stored by domestic service providers (e.g. through a domestic court order or a search warrant)? **MLA Act 2020**
Section 19 of the MLA Act of 2020 describes the procedure for the expedited preservation and disclosure of information systems upon request by a country. Section 20 in providing the procedure for the production, search and seizure of information systems, establishes that upon request of a country, the central authority may make an application to the court to issue an order for the production of: (a) specified electronic data in the possession or control of a person which is stored in a computer system and is reasonably believed to be connected with a criminal matter pending in the requesting country; and (b) electronic data in the possession or control of service provider, where such data or information is reasonably believed to be connected to criminal matter pending in the requesting country. The court may issue a search warrant or order authorizing a person designated by it to search or otherwise access any computer system or part thereof in which computer data may be stored.

Relevant for the execution of the request under domestic law is also Chapter 4 of the Act No. 1 2013 (Investigation for Fair Trial Act).

Powers and Procedures to execute a request under the national law:
The 1898 Code of Criminal Procedure (Amended in 2017), The Prevention of Electronic Crimes Ordinance of 2009 and the Prevention of Electronic Crimes Act of 2016 (PECA) are the legal bases for issuing an order for identification/ investigation (including trans-border access), retention and acquisition of data, metadata, traffic data, access data and content data. These provisions regulate the search and seizure of a computer system and the powers of the officer entitled to execute the warrant.
Under the 1898 Code of Criminal Procedure (Amendments to 16 February 2017) Section 94 a summons to produce document or other thing shall be issued whenever any Court, or, any officer in charge of a police-station considers that the production of any document or other thing is necessary or desirable for the purposes of any investigation, inquiry, trial or other proceeding.
Under the 2009 Prevention of Electronic Crimes Ordinance Chapter IV:

- Section 26 related to the Power of Officer in possession of a search warrant to have access to an electronic system or data information.
- Section 27 on real-time collection of traffic data.
- Section 28 is about retention of traffic data, according to which a service provider shall, within its existing or required technical capability, retain its traffic data minimum for a period of ninety days (90) and provide that data to the investigating agency or the investigating officer when required. The Federal Government may extend the period to retain such date as and when deems appropriate.
- Section 29 provides regulation for trans-border access for the purpose of investigation.

Under 2016 PECA, Chapter III provides the procedural powers for investigation:

- Section 26, establishes the investigation agency for the purposes of investigation of offences under this Act. The investigation agency shall establish its own capacity for forensic analysis of the data or information systems and the forensic analysis reports generated by the investigation agency shall not be inadmissible in evidence before any court for the sole reason that such reports were generated by the investigation agency.
- Section 27 sets out that the power to investigate under this Act entitles only to authorized officer of the investigation agency.
- Section 28 on explicated preservation and acquisition of data.
- Section 29 on retention of traffic data: a service provider shall, within its existing or required technical capability, retain its specified traffic data for a minimum period of one year or such period as the Authority may notify from time to time and, subject to production of a warrant issued by the court, provide that data to the investigation agency or the authorized officer whenever so required.
- Sections 30 and 31 establish the conditions to issue a warrant for search or seizure and the ones for disclosure of content data.

- Section 32 describes that an authorized officer is entitled to have access to any specified information system and demand any information in readable format; obtain copy of relevant data; require any person the officer has reasonable cause to believe to provide him reasonable technical and other assistance or to grant him access to data, device or information system in unencrypted or decrypted intelligible format. In exercise of the power of search and seizure of any information system, program or data […].
- Section 33, articulates how the authorized officer who conducted the search and seizure must deal with seized data or information systems.
- Section 36 indicates procedure for real-time collection and recording of information.
- Under Section 36 (4) confidentiality is expressed, requiring the designated agency to keep confidential the fact of the execution of any power provided for in this section and any information relating to it. Section 36 (5) provides the substantive grounds and reasons for real-time collection of data.

Can you provide assistance in real-time collection of non-content and/or content data (e.g. through electronic surveillance) upon the receipt of a MLA request? If yes, are there any limitations or conditions (e.g. limited to certain crime types or penalties thresholds)?

Due to section 29, International Cooperation, of the 2009 Prevention of Electronic Crimes Ordinance, the Federal Government has the power to investigate or proceed, collect, preserve, disclose. More specifically, "it may cooperate with any foreign Government, Interpol or any other international agency with whom it has or establishes reciprocal arrangements for the purposes of investigations or proceedings concerning offences related the electronic system and data, or for the collection of evidence in electronic form of an offence or obtaining expeditious preservation and disclosure of traffic data or data by means of an electronic system or real-time collection of traffic data associated with specified communications or interception of data.
Subject to the provisions of this Act, mutual legal assistance may be provided by Pakistan to a country on the principle of reciprocity reduced in writing. Thus, this provision can cover both outgoing and incoming requests.
Under the Mutual Legal Assistance (in Criminal Matters) Act of 2020, the request for data production is covered under section 19 of the MLA Act 2020, while the procedure for data production/execution is described under section 20 of the MLA Act 2020.

The 1898 Code of Criminal Procedure (Amended in 2017), The Prevention of Electronic Crimes Ordinance of 2009 and the Prevention of Electronic Crimes Act of 2016 (PECA) are the legal bases for issuing an order for identification/ investigation (including trans-border access), retention and acquisition of data, metadata, traffic data, access data and content data. These provisions regulate the search and seizure of a computer system and the powers of the officer entitled to execute the warrant.
Under the 2009 Prevention of Electronic Crimes Ordinance Chapter IV, Section 27 indicates the provision on real-time collection of traffic data.

Section 36 of the 2016 PECA, Chapter III, provides the procedural powers for investigation. Regarding real-time collection and recording of information is indicated that if the information furnished by an authorized officer satisfied the legal standards of reasonable ground to believe that the content of any information is reasonably required for the purpose of a specific criminal investigation, the Court may order, with respect to information held by or passing through a service provider, to a designated agency has notified under the Investigation for Fair Trial Act 2013 (I of 2013) or any other law for the time being in force having capability to collect real time information, such information in real-time in coordination with the investigation agency for provision in the prescribed manner. A real-time collection shall not be for a period beyond what is absolutely necessary and in any event for not more than seven days, period that might be extended by the Court.

What are the central and competent authorities in your country to:

a) Receive a request for MLA in criminal matters?

b) Execute/recognize the measure (if other than the receiving authority)?

As indicated under Section 4 of the MLA Act, the central authority shall have powers to perform duties and functions under this Act. Any references to "central authority" refer to the office of the secretary to the Ministry of the Interior of the Islamic Republic of Pakistan.

Furthermore, under the Prevention of Electronic Crimes Act, the Federal Government is the competent authority with respect to sending and receiving international cooperation requests.

Namely, as follows:

- Ministry of Interior (MLA on UNCTOC)
- National Accountability BUREAU (MLA on UNCAC)
- Anti-Narcotics Force;
- Ministry of Narcotics Control.

The competent authority to execute the request/decision for judicial cooperation is the same as the above. Section4 (3) of the MLA Act of 2020 specifies that the powers of the office shall be exercised by an executive committee comprising the following:

- the Secretary to the Ministry of Interior, Government of the Islamic Republic of Pakistan;
- the Secretary to the Ministry of Law and Justice, Government of the Islamic Republic of Pakistan;
- the Secretary to the Ministry of Foreign Affairs, Government of the Islamic Republic of Pakistan; and
- the Home Secretaries of all the four Provinces, namely Balochistan, Khyber Pakhtunkhwa, Punjab and Sindh, while the secretary to the Ministry of Interior of the Islamic Republic of Pakistan shall be its convener.

Additionally, Section 4 articulates that the central authority may, having regard to its functions and to exercise its powers efficiently, delegate its functions and powers to one or more subordinate officers at or above the rank of Joint Secretary.

What are the accepted languages for MLA requests?
Once the MLA request is completed it may be necessary to obtain a translation into an official language or one of the official languages of the requested State. In Pakistan English is accepted.
Can the request be submitted electronically to the central authority?
Yes, but only in the case of a direct threat to the national security of the country info@interior.gov.pk
Can the request be submitted directly to the central authority?
Yes, but only in the case of a direct threat to the national security of the country. Otherwise, requests should be submitted via diplomatic channels or inter-agency cooperation (in case of MoU).
What are the specific requirements (e.g. dual criminality, minimum penalty thresholds, etc.) that the requesting states have to meet under your domestic laws for MLA requests seeking for the provision of electronic evidence?
The criterion of reciprocity has to be respected.

5) REQUESTING ELECTRONIC EVIDENCE ACROSS BORDERS

5.1. **Direct requests** to foreign service providers

5.1.1. Requests for preservation

Pakistan
What legal framework(s) is/are applicable, if any?
Interpol laws and PECA 2016.
Which authority(ies) in your country is/are allowed to request data preservation to foreign service providers?
The Federal Investigation Agency within the Ministry of Interior.

If the requested foreign service providers are prohibited or limited to preserve the data, are there any alternative options to preserve the data, e.g. through police-to-police cooperation, specialized networks (e.g. G7/8 24/7 Network) or MLA?

The Pakistani legal framework to request international cooperation in criminal matters, including requesting for preservation, presents different instruments is as follows:

International treaties:

- 2000 United Nations Convention against Transnational Organized Crime (UNTOC) art. 18 (4) and (5);
- The United Nations Convention Against Corruption (2003) art. 43 and 46;

For countries who have neither ratified nor implemented the above-mentioned instruments, the following legal framework(s) can be applicable:

- Other bilateral treaties;
- Other multilateral treaties;
- Mutual legal Assistance (Criminal Matters) Act, 2020. Section 7, Mutual legal assistance request by Pakistan, provides the matters that can be the object of an outgoing request for mutual legal assistance issued by the central authority to a country subject to the applicable laws of such country.
- Where the Federal Government considers it expedient to provide mutual legal assistance in a criminal matter to a country which has not entered into a reciprocal agreement with Pakistan, it may, by notification in the official Gazette, direct that the provisions of this Act shall, subject to such modifications and conditions as may be specified therein, have effect to that country (Art. 3 (3) of the Mutual Legal Assistance Act, 2020).

For Commonwealth States:

- The Revised Harare Scheme 2011: The Commonwealth States have adopted alternate schemes for international cooperation based on domestic legislation rather than treaties, and these arrangements have been consolidated into the Scheme Relating to Mutual Assistance in Criminal Matters within the Commonwealth (the Harare Scheme, Paragraphs 1(5)(j) allows for obtaining electronic evidence).

The Harare Scheme is not a legally binding instrument or treaty per se, it is a voluntary arrangement which Commonwealth States are expected to implement through domestic legislation.

Additionally, the Ministry of Interior has issued SOP (standard operating procedure) No. 8/3/2020-Law dated 8 April 2020 for police-to-police cooperation. Several channels are available for police-to-police cooperation and for the exchange of police information and intelligence, but certain channels appear most relevant:

- the national competent authorities (which are in some States referred to as designated single points of contact),

- the channel of regional/international organs (e.g. INTERPOL National Central Bureau or 24/7 Networks), and - the liaison officer channel. The legal competence to begin and direct criminal investigations belongs to the National Response Centre for Cyber Crimes (NR3C) of the Federal Investigation Agency.
Can a court order or a search warrant be issued for data preservation by foreign service providers? If not, what are the reasons?
Yes, it can.

5.1.2. Requests for voluntary disclosure

Pakistan
What legal framework(s) is/are applicable, if any?
Any provision appears to be present under Pakistani legislation regarding voluntary disclosure of information to a foreign service provider.
Which authority(ies) in your country is/are allowed to request data disclosure to foreign service providers?
Federal Investigation Agency (FIA) and Anti-Narcotics Force (ANF).
If the requested foreign service providers are prohibited or limited to voluntarily disclose the data, are there any alternative options to obtain the data, e.g. through police-to-police cooperation, specialized networks (e.g. G7/8 24/7 Network) or MLA?
Same as above. Interpol and MLA.
Can a court order or a search warrant be issued for data disclosure by foreign service providers? If not, what are the reasons?
Yes, it can.

UNODC
United Nations Office on Drugs and Crime

5.2. Requests sent by your central authority for **Mutual Legal Assistance (MLA)**

Pakistan
What is your central authority to send requests for MLA in criminal matters?
As indicated under Section 4 of the MLA Act, the central authority shall have powers to perform duties and functions under this Act. Any references to “central authority” refer to the office of the secretary to the Ministry of the Interior of the Islamic Republic of Pakistan. Furthermore, under the Prevention of Electronic Crimes Act, the Federal Government is the competent authority with respect to sending and receiving international cooperation requests. Namely, as follows: - Ministry of Interior (MLA on UNCTOC) - National Accountability BUREAU (MLA on UNCAC) - Anti-Narcotics Force; - Ministry of Narcotics Control.
Are informal contacts with the central authority of the requested states allowed and used?
Federal Investigation Agency Telephone: (92) 51 9204128 24 hrs Telephone: (92) 51 9210086 Fax: (92) 51 9201472 Email: info@interior.gov.pk