Pakistan

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Table of contents

Version 04/05/2020

[reference to the provisions of the Budapest Convention]

This profile has been prepared by the Cybercrime Programme Office (C-PROC) of the Council of Europe in view of sharing information on cybercrime legislation and assessing the current state of implementation of the Budapest Convention on Cybercrime under national legislation. It does not necessarily reflect official positions of the State covered or of the Council of Europe.

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

State:	
Signature of the Budapest Convention:	N/A
Ratification/accession:	N/A

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data": For the purposes of this Convention: a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; c "service provider" means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service; d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service	The Prevention of Electronic Crimes Act, 2016: Definitions: **Information system** means an electronic system for creating, generating, sending, receiving, storing, reproducing, displaying, recording or processing any information; **Data** includes content data and traffic data; **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 to perform a function; **Service provider** includes a person who: (a) acts as a service provider in relation to sending, receiving, storing, processing or distribution of any electronic communication or the provision of other services in relation to electronic communication through an information system; (b) owns, possesses, operates, manages or controls a public switched network or provides telecommunication services; or (c) processes or stores data on behalf of such electronic communication service or users of such service; **Traffic data** includes data relating to a communication indicating its origin, destination, route, time, size, duration or type of service;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Chapter II – Measures to be taken at the national level	
Section 1 – Substantive criminal law	
Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems	
Article 2 – Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	The Prevention of Electronic Crimes Act, 2016: Section 3-**Unauthorized access to information system or data** Whoever with dishonest intention gains unauthorized access to any information system or data shall be punished with imprisonment for a term which may extend to three months or with fine which may extend to fifty thousand rupees or with both Section 6-**Unauthorized access to critical infrastructure information system or data** Whoever with dishonest intention gains unauthorized access to any critical infrastructure information system or data shall be punished with imprisonment which may extend to three years or with fine which may extend to one million rupees or with both.
Article 3 – Illegal interception Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	The Prevention of Electronic Crimes Act, 2016: Section 19-**Unauthorized interception** Whoever with dishonest intention commits unauthorized interception by technical means of: (a) any transmission that is not intended to be and is not open to the public, from or within an information system; or (b) electromagnetic emissions from an information system that are carrying data, shall be punished with imprisonment of either description for a term which may extend to two years or with fine which may extend to five hundred thousand rupees or with both.
Article 4 – Data interference 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	The Prevention of Electronic Crimes Act, 2016: Section 5-**Interference with information system or data** Whoever with dishonest intention interferes with or damages or causes to be interfered with or damages any part or whole of an information system or data shall be punished with imprisonment which may extend to two years or with fine which may extend to five hundred thousand rupees or with both.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Section 8-**Interference with critical infrastructure information system or data** Whoever dishonest intention interferes with or damages, or causes to be interfered with or damaged, any part or whole of a critical information system, or data, shall be punished with imprisonment which may extend to seven years or with fine which may extend to ten million rupees or with both Section 4-**Unauthorized copying or transmission of data** Whoever with dishonest intention and without authorization copies or otherwise transmits or causes to be transmitted any data shall be punished with imprisonment for a term which may extend to six months, or with fine which may extend to one hundred thousand rupees or with both. Section 7-**Unauthorized copying or transmission of critical infrastructure data** Whoever with dishonest intention and without authorization copies or otherwise transmits or causes to be transmitted any critical infrastructure data shall be punished with imprisonment for a term which may extend to five years, or with fine which may extend to five million rupees or with both.
Article 5 – System interference Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data	The Prevention of Electronic Crimes Act, 2016: Section 5-**Interference with information system or data** Whoever with dishonest intention interferes with or damages or causes to be interfered with or damages any part or whole of an information system or data shall be punished with imprisonment which may extend to two years or with fine which may extend to five hundred thousand rupees or with both. Section 8-**Interference with critical infrastructure information system or data** Whoever dishonest intention interferes with or damages, or causes to be interfered with or damaged, any part or whole of a critical information system, or data, shall be punished with imprisonment which may extend to seven years or with fine which may extend to ten million rupees or with both
Article 6 – Misuse of devices	The Prevention of Electronic Crimes Act, 2016: Section 15-**Making, obtaining, or supplying device for use in offence**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of: i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.	Whoever produces, makes, generates, adapts, exports, supplies, offers to supply or imports for use any information system, data or device, with the intent to be used or believing that it is primarily to be used to commit or to assist in the commission of an offence under this Act shall, without prejudice to any other liability that he may incur in this behalf, be punished with imprisonment for a term which may extend to six months or with fine which may extend to fifty thousand rupees or with both. Section 16-**Unauthorized use of identity information** (1) Whoever obtains, sells, possesses, transmits or uses another person's identity information without authorization shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to five million rupees, or with both. (2) Any person whose identity information is obtained, sold, possessed, used or transmitted may apply to the Authority for securing, destroying, blocking access or preventing transmission of identity information referred to in sub-section (1) and the Authority on receipt of such application may take such measures as deemed appropriate for securing, destroying or preventing transmission of such identity information.
Title 2 – Computer-related offences	
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic,	The Prevention of Electronic Crimes Act, 2016: Section 13-**Electronic forgery** (1) Whoever interferes with or uses any information system, device or data, with the intent to cause damage or injury to the public or to any person, or to make any illegal claim or title or to cause any person to part with property or to enter

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	into any express or implied contract, or with intent to commit fraud by any input, alteration, deletion, or suppression of data, resulting in unauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of the fact that the data is directly readable and intelligible or not, shall be punished with imprisonment of either description for a term which may extend to three years, or with fine which may extend to two hundred and fifty thousand rupees or with both. (2) Whoever commits offence under sub-section (1) in relation to a critical infrastructure information system or data shall be punished with imprisonment for a term which may extend to seven years or with fine which may extend to five million rupees or with both.
Article 8 – Computer-related fraud Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.	The Prevention of Electronic Crimes Act, 2016: Section 14-**Electronic fraud** Whoever with the intent for wrongful gain interferes with or uses any information system, device or data or induces any person to enter into a relationship or deceives any person, which act or omission is likely to cause damage or harm to that person or any other person shall be punished with imprisonment for a term which may extend to two years or with fine which may extend to ten million rupees or with both.
Title 3 – Content-related offences	
Article 9 – Offences related to child pornography 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system;	The Prevention of Electronic Crimes Act, 2016: Section 22-**Child pornography** (1) Whoever intentionally produces, offers or makes available, distributes or transmits through an information system or procures for himself or for another person or without lawful justification possesses material in an information system, that visually depicts, (a) a minor engaged in sexually explicit conduct; (b) a person appearing to be a minor engaged in sexually explicit conduct; or (c) realistic images representing a minor engaged in sexually explicit conduct; or (d) discloses the identity of the minor,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct 3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.	shall be punished with imprisonment for a term which may extend to seven years, or with fine which may extend to five million rupees or with both. (2) Any aggrieved person or his guardian, where such person is a minor, may apply to the Authority for removal, destruction of or blocking access to such information referred to in sub-section (1) and the Authority, on receipt of such application, shall forthwith pass such orders as deemed reasonable in the circumstances, including an order for removal, destruction, preventing transmission of or blocking access to such information and the Authority may also direct any of its licensees to secure such information including traffic data. **Penal Code** Section 292-**Sale, etc., of obscene books, etc.:** Whoever: (a) sells, lets to hire, distributes, publicly exhibits or in any manner puts into circulation, or for purposes of sale. hire, distribution, public exhibition or circulation,, makes, produces or has in his possession any obscene book, pamphlet, paper, drawing, painting, representation or figure or any other obscene object whatsoever, or (b) imports, exports or conveys any obscene object for any of the purposes aforesaid, or knowing or having reason to believe that such object will be sold, let to hire, distributed or publicly exhibited or in any manner put into circulation, or shall be punished with imprisonment of either description for a term which may extend to six months, or with fine which may extend to one thousand rupees, or with both. (c) takes part in or receives profits from, any business in the course of which he knows or has reason to believe that any such obscene objects are, for any of -the purposes aforesaid, made, produced, purchased, kept, imported, exported, conveyed, publicly exhibited or in any manner put into circulation, or . (d) advertises or makes known by any means whatsoever that any person he engaged or is ready to engage in any act which is an offence under this section, or that any such obscene object can be procured from or through any person, or (e) offers or attempts to do any act which is an offence under this section, shall be punished with imprisonment of either description for a term which may extend to three months, or which tine or with both.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Exception: This section does not extend to any book, pamphlet, writing, drawing or painting kept or used bona fide for religious purposes or any representation sculptured, engraved, painted or otherwise represented on or in any temple, or on any car used for the conveyance of idols, or kept or used for any religious purpose.
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	The Copyright Ordinance, 1962 **66. Offences of infringement of copyright or the other rights conferred by this Ordinance.-** 1. Any person who knowingly infringes or abets the infringement of __ (a) the copyright in a work, (ab) the rental rights in cinematographic works and computer programmes; (ac) the rights of performers or producers of sound recording; or (b) any other right conferred by this Ordinance, shall be punishable with imprisonment which may extend to three years, or with fine which may extend to one hundred thousand rupees or with both.
Title 5 – Ancillary liability and sanctions	
Article 11 – Attempt and aiding or abetting	The Prevention of Electronic Crimes Act, 2016:

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention. 3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	Section 28-**Pakistan Penal Code, 1860 (Act XLV of 1860) to apply.** The provisions of the Pakistan Penal Code, 1860 (Act XLV of 1860), to the extent not inconsistent with anything provided in this Act, shall apply to the offences provided in this Act. Penal Code Section 34-**Acts done by several persons** In furtherance of common intention. When a criminal act is done by several persons, in furtherance of the common intention of all, each such person is liable for that act in the same manner as if it were done by him alone. Section 109-**Punishment of abetment if the Act abetted committed In consequence and where no express provision is made for its punishment** Whoever abets any offence shall, if the act abetted is committed in consequence of the abetment, and no express provision is made by this Code, for the punishment of such abetment, be punished with the punishment provided for the offence: Provided that, except in case of Ikrah-i-Tam, the, abettor of an offence referred to in Chapter XVI shall be liable to punishment of ta'zir specified for such offence including death. Explanation: An act or offence is said-to be committed in consequence of abetment, when it is committed in consequence of the instigation, or in pursuance of the conspiracy, or with the aid which constitutes the abetment. **Section 511-Punishment for attempting to commit offences punishable with imprisonment for life or for a shorter terms** Whoever attempts to commit an offence punishable by this Code with imprisonment for life or imprisonment, or to cause such an offence to be committed, and in such attempt does any act towards the commission of the offence, shall where no express provision is made by this Code for the punishment of such attempt, be punished with imprisonment of any description provided for the offence for a term which may extend to one-half of the longest term of imprisonment provided for that offence or with such fine daman as is provided for the offence, or with both.
Article 12 – Corporate liability 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by	The Prevention of Electronic Crimes Act, 2016: Section 28-**Pakistan Penal Code, 1860 (Act XLV of 1860) to apply.**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a a power of representation of the legal person; b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority. 3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	The provisions of the Pakistan Penal Code, 1860 (Act XLV of 1860), to the extent not inconsistent with anything provided in this Act, shall apply to the offences provided in this Act. Penal Code Section 11-**"Person"** The word "person" includes any Company or Association, or body of persons, whether incorporated or not.
Article 13 – Sanctions and measures 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty. 2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.	
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.	The Prevention of Electronic Crimes Act, 2016: Section 35**- Powers of an authorized officer** (1) Subject to provisions of this Act, an authorized officer shall have the powers to: (a) have access to and inspect the operation of any specified information system; (b) use or cause to be used any specified information system to search any specified data contained in or available to such system; (c) obtain and copy only relevant data, use equipment to make copies and obtain an intelligible output from an information system; (d) have access to or demand any information in readable and comprehensible format or plain version; (e) require any person by whom or on whose behalf, the authorized officer has reasonable cause to believe, any information system has been used to grant access to any data within an information system within the control of such person;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	(f) require any person having charge of or otherwise concerned with the operation of any information system to provide him reasonable technical and other assistance as the authorized officer may require for investigation of an offence under this Act; and (g) require any person who is in possession of decryption information of an information system, device or data under investigation to grant him access to such data, device or information system in unencrypted or decrypted intelligible format for the purpose of investigating any such offence: *Explanation:*Decryption information means information or technology that enables a person to readily retransform or unscramble encrypted data from its unreadable form and from ciphered data to intelligible data. (2) In exercise of the power of search and seizure of any information system, program or data the authorized officer at all times shall, (a) act with proportionality; (b) take all precautions to maintain integrity and secrecy of the information system and data in respect of which a warrant for search or seizure has been issued; (c) not disrupt or interfere with the integrity or running and operation of any information system or data that is not the subject of the offences identified in the application for which a warrant for search or seizure has been issued; (d) avoid disruption to the continued legitimate business operations and the premises subjected to search or seizure under this Act; and (e) avoid disruption to any information system, program or data not connected with the information system that is not the subject of the offences identified in the application for which a warrant has been issued or is not necessary for the investigation of the specified offence in respect of which a warrant has been issued. (3) When seizing or securing any data or information system, the authorized officer shall make all efforts to use technical measures to maintain its integrity and chain of custody. The authorized officer shall seize an information system, data, device or articles, in part or in whole, as a last resort only in the event where it is not possible under the circumstances to use such technical measures or where use of such technical measures by themselves shall not be sufficient to maintain the integrity and chain of custody of the data or information system being seized. (4) Where an authorized officer seizes or secures any data or information system, the authorized officer shall ensure that data or information system while in the possession or in the access of the authorized officer is not released to any other

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	person including competitors or public at large and details including log of any action performed on the information system or data is maintained in a manner prescribed under this Act. Section 34**-Warrant for disclosure of content data** (1) Upon an application by an authorised officer that demonstrates to the satisfaction of the Court that there exist reasonable grounds to believe that the content data stored in an information system is reasonably required for the purpose of a criminal investigation or criminal proceedings with respect to an offence made out under this Act, the Court may, after recording reasons, order that the person in control of the data or information system, to provide such data or access to such data to the authorized officer. (2) The period of a warrant issued under sub-section (1) may be extended beyond seven days if, an application, a Court authorizes an extension for a further period of time as may be specified by the Court.
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.	The Prevention of Electronic Crimes Act, 2016: **Section 31-Expedited preservation and acquisition of data.** (1) If an authorized officer is satisfied that: (a) specific data stored in any information system or by means of an information system is reasonably required for the purposes of a criminal investigation; and (b) there is a risk or vulnerability that the data may be modified, lost, destroyed or rendered inaccessible, the 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 days as specified in the notice: Provided that the authorized officer shall immediately but not later than twenty-four hours bring to the 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. (2) The period provided in sub-section (1) 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.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 17 – Expedited preservation and partial disclosure of traffic data 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	The Prevention of Electronic Crimes Act, 2016: **Section 31-Expedited preservation and acquisition of data.** (1) If an authorized officer is satisfied that: (a) specific data stored in any information system or by means of an information system is reasonably required for the purposes of a criminal investigation; and (b) there is a risk or vulnerability that the data may be modified, lost, destroyed or rendered inaccessible, the 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 days as specified in the notice: Provided that the authorized officer shall immediately but not later than twenty-four hours bring to the 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. (2) The period provided in sub-section (1) 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.
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is	The Prevention of Electronic Crimes Act, 2016: **Section 31-Expedited preservation and acquisition of data.** (1) If an authorized officer is satisfied that: (a) specific data stored in any information system or by means of an information system is reasonably required for the purposes of a criminal investigation; and (b) there is a risk or vulnerability that the data may be modified, lost, destroyed or rendered inaccessible, the 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 days as specified in the notice: Provided that the authorized officer shall immediately but not later than twenty-four hours bring to the 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

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	appropriate in the circumstances of the case including issuance of warrants for retention of such data or otherwise. (2) The period provided in sub-section (1) 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.
Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system.	The Prevention of Electronic Crimes Act, 2016: Section 33**-Warrant for search or seizure** (1) Upon an application by an authorized officer that demonstrates to the satisfaction of the Court that there exist reasonable grounds to believe that there may be in a specified place an information system, data, device or other articles that: (a) may reasonably be required for the purpose of a criminal investigation or criminal proceedings which may be material as evidence in proving a specifically identified offence made out under this Act; or (b) has been acquired by a person as a result of the commission of an offence, the Court may issue a warrant which shall authorize an officer of the investigation agency, with such assistance as may be necessary, to enter the specified place and to search the premises and any information system, data, device or storage medium relevant to the offence identified in the application and access, seize or similarly secure any information system, data, device or other articles relevant to the offence identified in the application. (2) In circumstances involving an offence under section 10, under which a warrant may be issued but cannot be obtained without the apprehension of destruction, alteration or loss of data, information system, data, device or other articles required for investigation, the authorized officer, who shall be a Gazetted officer of the investigation agency, may enter the specified place and search the premises and any information system, data, device or other articles relevant to the offence and access, seize or similarly secure any information system, data, device or other articles relevant to the offence:

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	Provided that the authorized officer shall immediately but not later than twenty-four hours bring to the notice of the Court, the fact of such search or seizure and the Court on receipt of such information may pass such orders as deemed appropriate in the circumstances of the case. Section 35-**Powers of an authorized officer** (1) Subject to provisions of this Act, an authorized officer shall have the powers to— (a) have access to and inspect the operation of any specified information system; (b) use or cause to be used any specified information system to search any specified data contained in or available to such system; (c) obtain and copy only relevant data, use equipment to make copies and obtain an intelligible output from an information system; (d) have access to or demand any information in readable and comprehensible format or plain version; (e) require any person by whom or on whose behalf, the authorized officer has reasonable cause to believe, any information system has been used to grant access to any data within an information system within the control of such person; (f) require any person having charge of or otherwise concerned with the operation of any information system to provide him reasonable technical and other assistance as the authorized officer may require for investigation of an offence under this Act; and (g) require any person who is in possession of decryption information of an information system, device or data under investigation to grant him access to such data, device or information system in unencrypted or decrypted intelligible format for the purpose of investigating any such offence:--- Explanation.—Decryption information means information or technology that enables a person to readily retransform or unscramble encrypted data from its unreadable form and from ciphered data to intelligible data. (2) In exercise of the power of search and seizure of any information system, program or data the authorized officer at all times shall,--- (a) act with proportionality; (b) take all precautions to maintain integrity and secrecy of the information system and data in respect of which a warrant for search or seizure has been issued;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(c) not disrupt or interfere with the integrity or running and operation of any information system or data that is not the subject of the offences identified in the application for which a warrant for search or seizure has been issued; (d) avoid disruption to the continued legitimate business operations and the premises subjected to search or seizure under this Act; and (e) avoid disruption to any information system, program or data not connected with the information system that is not the subject of the offences identified in the application for which a warrant has been issued or is not necessary for the investigation of the specified offence in respect of which a warrant has been issued. (3) When seizing or securing any data or information system, the authorized officer shall make all efforts to use technical measures to maintain its integrity and chain of custody. The authorized officer shall seize an information system, data, device or articles, in part or in whole, as a last resort only in the event where it is not possible under the circumstances to use such technical measures or where use of such technical measures by themselves shall not be sufficient to maintain the integrity and chain of custody of the data or information system being seized. (4) Where an authorized officer seizes or secures any data or information system, the authorized officer shall ensure that data or information system while in the possession or in the access of the authorized officer is not released to any other person including competitors or public at large and details including log of any action performed on the information system or data is maintained in a manner prescribed under this Act. Section 36-Dealing with seized data or information system (1) If any data or information system has been seized or secured following a search or seizure under this Act, the authorized officer who undertook the search or seizure shall, at the time of the seizure,--- (a) make a list of what has been seized or rendered inaccessible, with the date and time of seizure; and (b) give a copy of that list to,--- (i) the occupier of the premises; or (ii) the owner of the data or information system; or (iii) the person from whose possession the data or information system has been seized, in a prescribed manner in the presence of two witnesses.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(2) The authorized officer, upon an application of the owner of the data or information system or an authorized agent of the owner and on payment of prescribed costs, shall provide forensic image of the data or information system to the owner or his authorized agent within a time prescribed under this Act. (3) If the authorized officer has reasons to believe that providing forensic image of the data or information system to the owner under sub-section (2) may prejudice,--- (a) the investigation in connection with which the search was carried out; or (b) another ongoing investigation; or (c) any criminal proceedings that are pending or that may be brought in relation to any of those investigations, the authorized officer shall, within seven days of receipt of the application under sub-section (2), approach the Court for seeking an order not to provide copy of the seized data or information system. (4) The Court, upon receipt of an application from an authorized officer under sub-section (3), may after recording reasons in writing pass such order as deemed appropriate in the circumstances of the case. (5) The costs associated with the exercise of rights under this section shall be borne by the person exercising these rights.
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.	The Prevention of Electronic Crimes Act, 2016: Section 39**-Real-time collection and recording of information.** (1) If a Court is satisfied on the basis of information furnished by an authorized officer that there are reasonable grounds to believe that the content of any information is reasonably required for the purposes 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 as 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, to collect or record such information in real-time in coordination with the investigation agency for provision in the prescribed manner: Provided that such real-time collection or recording shall not be ordered for a period beyond what is absolutely necessary and in any event for not more than seven days. (2) Notwithstanding anything contained in any law to the contrary the information so collected under sub-section (1) shall be admissible in evidence. (3) The period of real-time collection or recording may be extended beyond seven days if, on an application, the Court authorizes an extension for a further specified period.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	(4) The Court may also require 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. (5) The application under sub-sections (1) and (2) shall in addition to substantive grounds and reasons also: (a) explain why it is believed that the data sought will be available with the person in control of an information system; (b) identify and explain with specificity the type of information likely to be found on such information system; (c) identify and explain with specificity the identified offence made out under this Act in respect of which the warrant is sought; (d) if authority to seek real-time collection or recording on more than one occasion is needed, explain why and how many further disclosures are needed to achieve the purpose for which the warrant is to be issued; (e) specify what measures shall be taken to prepare and ensure that the real-time collection or recording is carried out whilst maintaining the privacy of other users, customers and third parties and without the disclosure of information of any person not part of the investigation; (f) explain why the investigation may be frustrated or seriously prejudiced unless the real time collection or recording is permitted; and (g) why, to achieve the purpose for which the warrant is being applied, real time collection or recording by the person in control of the information system is necessary.
Article 21 – Interception of content data 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt	The Prevention of Electronic Crimes Act, 2016: Section 39**-Real-time collection and recording of information.** (1) If a Court is satisfied on the basis of information furnished by an authorized officer that there are reasonable grounds to believe that the content of any information is reasonably required for the purposes 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 as 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, to collect or record such information in real-time in coordination with the investigation agency for provision in the prescribed manner: Provided that such real-time collection or recording shall not be ordered for a period beyond what is absolutely necessary and in any event for not more than seven days.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	(2) Notwithstanding anything contained in any law to the contrary the information so collected under sub-section (1) shall be admissible in evidence. (3) The period of real-time collection or recording may be extended beyond seven days if, on an application, the Court authorizes an extension for a further specified period. (4) The Court may also require 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. (5) The application under sub-sections (1) and (2) shall in addition to substantive grounds and reasons also: (a) explain why it is believed that the data sought will be available with the person in control of an information system; (b) identify and explain with specificity the type of information likely to be found on such information system; (c) identify and explain with specificity the identified offence made out under this Act in respect of which the warrant is sought; (d) if authority to seek real-time collection or recording on more than one occasion is needed, explain why and how many further disclosures are needed to achieve the purpose for which the warrant is to be issued; (e) specify what measures shall be taken to prepare and ensure that the real-time collection or recording is carried out whilst maintaining the privacy of other users, customers and third parties and without the disclosure of information of any person not part of the investigation; (f) explain why the investigation may be frustrated or seriously prejudiced unless the real time collection or recording is permitted; and (g) why, to achieve the purpose for which the warrant is being applied, real time collection or recording by the person in control of the information system is necessary.
Section 3 – Jurisdiction	
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or	Section 1-**Short title, extent, application and commencement.** (2) It extends to the whole of Pakistan. (3) It shall apply to every citizen of Pakistan wherever he may be and also to every other person for the time being in Pakistan. (4) It shall also apply to any act committed outside Pakistan by any person if the act constitutes an offence under this Act and affects a person, property, information system or data located in Pakistan.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	
Chapter III – International co-operation	
Article 24 – Extradition 1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply. 2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article. 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party. 7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure	
Article 25 – General principles relating to mutual assistance 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.	The Prevention of Electronic Crimes Act, 2016: Section 42**-International cooperation** (4) The Federal Government may, through the designated agency, send and answer requests for mutual assistance the execution of such requests or their transmission to the authorities competent for their execution.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35. 3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.	(5) The Federal Government may refuse to accede to any request made by a foreign government, 24 x 7 network, any foreign agency or any international organization or agency, if (a) it is of the opinion that the request, if granted, would prejudice sovereignty, security, public order or other essential public interest of Pakistan; (b) the offence is regarded by the Federal Government as being of a political nature; (c) there are substantial grounds for believing that the request for assistance has been made for the purpose of prosecuting a person on account of that person's race, sex, religion, nationality, ethnic origin or political opinions or that that person's position may be prejudiced for any of those reasons; (d) the request relates to an offence the prosecution of which in the requesting State may be incompatible with the laws of Pakistan; (e) the assistance requested requires the Federal Government to carry out compulsory measures that may be inconsistent with the laws or practices of Pakistan had the offence been the subject of investigation or prosecution under its own jurisdiction; or (f) the request concerns an offence which may prejudice an ongoing investigation or trial or rights of its citizens guaranteed under the Constitution. (5) The Federal Government may refuse to accede to any request made by a foreign government, 24 x 7 network, any foreign agency or any international organization or agency, if (a) it is of the opinion that the request, if granted, would prejudice sovereignty, security, public order or other essential public interest of Pakistan; (b) the offence is regarded by the Federal Government as being of a political nature; (c) there are substantial grounds for believing that the request for assistance has been made for the purpose of prosecuting a person on account of that person's race, sex, religion, nationality, ethnic origin or political opinions or that that person's position may be prejudiced for any of those reasons; (d) the request relates to an offence the prosecution of which in the requesting State may be incompatible with the laws of Pakistan; (e) the assistance requested requires the Federal Government to carry out compulsory measures that may be inconsistent with the laws or practices of Pakistan had the offence been the subject of investigation or prosecution under its own jurisdiction; or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(f) the request concerns an offence which may prejudice an ongoing investigation or trial or rights of its citizens guaranteed under the Constitution.
Article 26 – Spontaneous information 1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter. 2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	The Prevention of Electronic Crimes Act, 2016: Section 42**-International cooperation** (2) The Federal Government may forward to a foreign government, 24x7 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.
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times. 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party. 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities. 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary. 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly. 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party. b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so. d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party. e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.	
Article 28 – Confidentiality and limitation on use 1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or b not used for investigations or proceedings other than those stated in the request. 3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it. 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.	The Prevention of Electronic Crimes Act, 2016: Section 42**-International cooperation** (3) The Federal Government shall require the foreign government, 24 x 7 netwo rk, any foreign agency or any international organization or agency to keep the information provided confidential and use it strictly for the purposes it is provided.
Article 29 – Expedited preservation of stored computer data	The Prevention of Electronic Crimes Act, 2016 Section 42**-International cooperation**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data. 2 A request for preservation made under paragraph 1 shall specify: a the authority seeking the preservation; b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; c the stored computer data to be preserved and its relationship to the offence; d any available information identifying the custodian of the stored computer data or the location of the computer system; e the necessity of the preservation; and f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data. 3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation. 4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. 5 In addition, a request for preservation may only be refused if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	(1) The Federal Government may upon receipt of a request, through the designated agency under this Act, extend such cooperation 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.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 4 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.	
Article 30 – Expedited disclosure of preserved traffic data 1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted. 2 Disclosure of traffic data under paragraph 1 may only be withheld if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	The Prevention of Electronic Crimes Act, 2016 Section 42**-International cooperation** (1) The Federal Government may upon receipt of a request, through the designated agency under this Act, extend such cooperation 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.
Article 31 – Mutual assistance regarding accessing of stored computer data 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where:	The Prevention of Electronic Crimes Act, 2016 Section 42**-International cooperation** (1) The Federal Government may upon receipt of a request, through the designated agency under this Act, extend such cooperation 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.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	
Article 32 – Trans-border access to stored computer data with consent or where publicly available A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	
Article 33 – Mutual assistance in the real-time collection of traffic data 1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	The Prevention of Electronic Crimes Act, 2016 Section 42**-International cooperation** (1) The Federal Government may upon receipt of a request, through the designated agency under this Act, extend such cooperation 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.
Article 34 – Mutual assistance regarding the interception of content data The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.	The Prevention of Electronic Crimes Act, 2016 Section 42**-International cooperation** (1) The Federal Government may upon receipt of a request, through the designated agency under this Act, extend such cooperation 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.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 35 – 24/7 Network 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects. 2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis. 3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.	The Prevention of Electronic Crimes Act, 2016 Section 42**-International cooperation** (4) The Federal Government may, through the designated agency, send and answer requests for mutual assistance the execution of such requests or their transmission to the authorities competent for their execution.
Article 42 – Reservations By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.	

Back to the Table of Contents