SERBIA

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Table of contents

Version 6 April 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:	07/04/2005
Ratification/accession:	14/04/2009

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.	**Criminal Code Art. 112 – meaning of the terms** (34) A **computer system** shall mean any device or a group of interconnected or dependent devices of which one or more of them carry out automatic data processing by means of computer software. (17) **Computer data** is any representation of facts, information, or concepts in the form suitable for processing by a computer, including as well appropriate computer software necessary for the functioning of a computer. **Law on Electronic Communications Art. 4 – definition of terms** 30) operator is an entity which performs or is authorized to perform activities within the electronic communications sector
Section 1 – Substantive criminal law	
Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems	
Article 2 – Illegal access	**Criminal Code Art. 302 - Unauthorised Access to Computer, Computer**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**Network or Electronic Data Processing** (1) Whoever, by circumventing protection measures, accesses a computer or computer network without authorisation, or accesses electronic data processing without authorisation, shall be punished by fine or imprisonment up to six months. (2) Whoever records or uses data obtained in manner provided under paragraph 1 of this Article, shall be punished by fine or imprisonment up to two years. (3) If the offence specified in paragraph 1 of this Article results in hold-up or serious malfunction in electronic processing and transfer of data or of the network, or other grave consequences have resulted, the offender shall be punished by imprisonment up to three years. **Criminal Code Art. 304 - Unauthorised Use of Computer of Computer Network** (1) Whoever uses computer services or computer network with intent to acquire unlawful material gain for himself or another, shall be punished by fine or imprisonment up to three months. (2) Prosecution for the offence specified in paragraph 1 of this Article shall be instigated by private action.
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.	**Criminal Code Art. 142 – Violation of Privacy of Letter and other Mail** (1) Whoever without authorisation opens another's letter, telegram or other closed correspondence or consignment or otherwise violates their privacy or whoever without authorisation withholds, conceals, destroys or delivers to other person somebody else's letter, telegram or other mail or who violates the privacy of electronic mail, shall be punished with fine or imprisonment up to two years. (2) The penalty specified in paragraph 1 of this Article shall be imposed also to whoever communicates to another the content of another's closed mail, telegram or consignment acquired by violating the privacy thereof, or makes use of such contents. (3) If the offence specified in paragraphs 1 and 2 of this Article is committed by an official in discharge of duty, such person shall be punished with imprisonment from six months to three years.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Criminal Code Art. 143 – Unauthorised Wiretapping and Recording (1) Whoever using special equipment taps or records conversation, statement or announcement that is not intended for him, shall be punished with fine or imprisonment from three months to three years. (2) The penalty specified in paragraph 1 of this Article shall be imposed also on whoever enables an unknown person to be informed with the conversation, statement or announcement obtained through unauthorised tapping or audio recording. (3) if the offence specified in paragraphs 1 and 2 of this Article is committed by an official in discharge of duty, such person shall be punished with imprisonment from six months to five years. **Criminal Code Art. 146 – Unauthorised Collection of Personal Data** (1) Whoever without authorisation obtains, communicates to another or otherwise uses information that is collected, processed and used in accordance with law, for purposes other than those for which they are intended, shall be punished with a fine or imprisonment up to one year. (2) The penalty specified in paragraph 1 of this Article shall also be imposed on whomever contrary to law collects personal data on citizens and uses data so collected. (3) If the offence specified in paragraph 1 of this Article is committed by an official in discharge of duty, such person shall be punished with imprisonment up to three years.
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.	**Criminal Code Art. 298 - Damaging Computer Data and Programs** (1) Whoever without authorisation deletes, alters, damages, conceals or otherwise makes unusable a computer datum or program, shall be punished by fine or imprisonment up to one year. (2) If the offence specified in paragraph 1 of this Article results in damages exceeding four hundred and fifty thousand dinars, the offender shall be punished by imprisonment of three months to three years.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(3) If the offence specified in paragraph 1 of this Article results in damages exceeding one million five hundred thousand dinars, the offender shall be punished by imprisonment of three months to five years. (4) Equipment and devices used in perpetration of the offence specified in paragraphs 1 and 2 of this Article shall be seized.
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.	**Criminal Code Art. 299 – Computer Sabotage** Whoever enters, destroys, deletes, alters, damages, conceals or otherwise makes unusable computer datum or program or damages or destroys a computer or other equipment for electronic processing and transfer of data, with intent to prevent or considerably disrupt the procedure of electronic processing and transfer of data that are of importance for government authorities, enterprises or other entities, shall be punished by imprisonment of six months to five years. **Criminal Code Art. 303 – Preventing or Restricting Access to Public Computer Network** (1) Whoever without authorisation prevents or hinders access to a public computer network, shall be punished by fine or imprisonment up to one year. (2) If the offence specified in paragraph 1 of this Article is committed by an official in discharge of duty, such official shall be punished by imprisonment up to three years.
Article 6 – Misuse of devices 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,	**Criminal Code Art. 300 – Creating and Introducing of Computer Viruses** (1) Whoever makes a computer virus with intent to introduce it into another's computer or computer network, shall be punished by fine or imprisonment up to six months. (2) Whoever introduces a computer virus into another's computer or computer network thereby causing damage, shall be punished by fine or imprisonment up to two years. (3) Equipment and devices used for committing of the offence specified in paragraphs 1 and 2 of this Article shall be seized.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**Criminal Code Art. 304a – Manufacture, Procurement, and Provision to others of Means of Committing Criminal Offences against Security of Computer Data** (1) Whoever possesses, manufactures, procures, sells, or gives to others for their use computers, computer systems, computer data or software intended for committing one of the criminal offences referred to in Articles 298 through 303 herein shall be punished with imprisonment of six months to three years. (2) Items referred to in paragraph 1 hereof shall be seized.
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, 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.	**Criminal Code Art. 355 – Forging a Document** (1) Whoever makes a forged document or alters a real document with intent to use such document as real or uses a forged or altered document as real or obtains such document to use, shall be punished by imprisonment up to three years. (2) If the offence specified in paragraph 1 of this Article is committed in respect of a public document, testament, bill of exchange, cheque, public or official record or other record that is kept under law, the offender shall be punished by imprisonment of three months to five years. (3) The attempt of the offence specified in paragraph 1 of this Article shall be punished. **Criminal Code Art. 356 – Special Cases of Forging Documents** The following shall be deemed to be forging documents and shall be punished pursuant to Article 355 hereof:

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	1) whoever without authorisation fills in a statement having affect as legal instrument in legal relations by using a blank form, paper or other document signed by another; 2) Whoever deceives another in respect of content of a document and such party affixes their signature on such document believing that he/she is signing another document or another content; 3) whoever issues a document on behalf of another without authorisation of that person or on behalf of a person who does not exist; 4) whoever as an issuer of a document affixes with his signature a position, rank or title although he holds no such position, rank or title, thereby granting crucial force of evidence to such document; 5) whoever produces a document by using a genuine seal or sign without authorisation. **Criminal Code Art. 357 – Forging an Official Document** (1) An official who enters false data or fails to enter important data in an official document, record or file, or who certifies by his signature or official seal an official document, record or file with false content, or who with his signature or official seal enables another to produce an official document, record or file with false content, shall be punished by imprisonment of three months to five years. (2) The penalty specified in paragraph 1 of this Article shall also be imposed to an official who in service uses a forged document, record or file as true, or who destroys, conceals or considerably damages an official document, record or file or makes it otherwise unusable. (3) The responsible officer in an enterprise, institution or other entity who commits the offence specified in paragraphs 1 and 2 of this Article shall be punished by the penalty prescribed for that offence.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**Criminal Code Art. 301 – Computer Fraud** (1) Whoever enters incorrect data, fails to enter correct data or otherwise conceals or falsely represents data and thereby affects the results of electronic processing and transfer of data with intent to acquire for himself or another unlawful material gain and thus causes material damage to another person, shall be punished by fine or imprisonment up to three years. (2) If the offence specified in paragraph 1 of this Article results in acquiring material gain exceeding four hundred and fifty hundred thousand dinars, the offender shall be punished by imprisonment of one to eight years. (3) If the offence specified in paragraph 1 of this Article results in acquiring material gain exceeding one million five hundred thousand dinars, the offender shall be punished by imprisonment of two to ten years. (4) Whoever commits the offence specified in paragraph 1 of this Article from malicious mischief, shall be punished by fine or imprisonment up to six months. **Criminal Code Art. 304 – Unauthorised Use of Computer of Computer Network** (1) Whoever uses computer services or computer network with intent to acquire unlawful material gain for himself or another, shall be punished by fine or imprisonment up to three months. (2) Prosecution for the offence specified in paragraph 1 of this Article shall be instigated by private action.
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;	**Criminal Code Art. 185 – Showing, procuring and possession of Pornographic Material and Juvenile Pornography** (1) Whoever sells, shows or publicly displays or otherwise makes available texts, pictures, audio-visual or other items of pornographic content to a minor or shows to a child a pornographic performance, shall be punished with a fine or imprisonment up to six months.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
c distributing or transmitting child pornography through a computer system; 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.	(2) Whoever uses a minor to produce photographs, audio-visual or other items of pornographic content or for a pornographic show, shall be punished with imprisonment from six months to five years. (3) If the offence referred to in paragraphs 1 and 2 hereof has been perpetrated against a child, the offender shall be punished with imprisonment of six months to three years for the offence from paragraph 1 and with imprisonment of one year to eight years for the offence from paragraph 2. (4) Whoever obtains for himself or another, possesses, sells, shows, publicly exhibits or electronically or otherwise makes available pictures, audio-visual or other items of pornographic content resulting abuse of a juvenile, shall be punished with imprisonment from three months to three years. (6) Items specified in paragraphs 1 through 4 of this Article shall be confiscated.
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.	**Criminal Code Art. 198 – Violation of Moral Right of Author and Performer** (1) Whoever under his name or the name of another publishes or puts into circulation copies of another's copyrighted work or performance or otherwise publicly presents another's copyrighted work or performance, in entirety or in part, shall be punished with a fine or imprisonment up to three years. (2) Whoever without the author's permission alters or adapts another's copyrighted work or alters another's recorded performance, shall be punished with a fine or imprisonment up to one year. (3) Whoever puts into circulation copies of another's copyrighted work or performance in a manner insulting the honour and reputation of the author or performer, shall be punished with a fine or imprisonment up to six months.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(4) Things referred to under paragraphs 1 through 3 of this Article shall be seized. (5) Prosecution for offences specified in paragraph 2 of this Article is initiated by the prosecution, and for offences referred to in paragraph 3 of this Article by private action. **Criminal Code Art. 199 – Unauthorised Use of Copyrighted Work or other Work Protected by Similar Right** (1) Whoever without permission publishes, records, copies or otherwise presents in public, in part or entirety, a copyrighted work, performance, phonogram, videogram, show, computer programme or database, shall be punished with a fine or imprisonment up to three years. (2) The punishment specified in paragraph 1 of this Article shall also be imposed on a person who puts into circulation, possesses or with intent to put into circulation illegally multiplied or illegally put into circulation copies of copyrighted work, performance, phonogram, videogram, show, computer program or database. (3) If the offence referred to in paragraphs 1 and 2 of this Article was committed with intent to acquire material gain for oneself or another, the offender shall be punished with imprisonment from six months to five years. (4) Whoever produces, imports, puts into circulation, sells, rents, advertises for sale or renting, or keeps for commercial purposes, equipment and devices whose basic or prevailing purpose is to remove, bypass or forestall technological measures intended for prevention of violation of copyright and other similar rights, or who uses such equipment or devices with an aim to violate copyright or other similar right, shall be punished with a fine or imprisonment up to three years. (5) The things referred to in paragraphs 1 through 4 shall be seized and destroyed. **Criminal Code Art. 200 – Unauthorised Removal or Altering of Electronic Information on Copyright and Similar Rights** (1) Whoever without authorisation removes or alters electronic information on copyright or other similar right, or puts into circulation, imports, exports,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	broadcasts or otherwise presents in public a copyrighted work or other work protected by similar right, from which electronic information on rights was removed or altered without authorisation, shall be punished with a fine and imprisonment up to three years. (2) The things referred to in paragraph 1 shall be seized and destroyed. **Criminal Code Art. 201 – Violation of Patent Rights** (1) Whoever without permission produces, imports, exports, offers for circulation, puts into circulation, stores or uses for commercial operations a patented product or procedure, shall be punished with a fine or imprisonment up to three years. (2) If the offence referred to in paragraph 1 results in material gain or damage in an amount exceeding one million dinars, the offender shall be punished with imprisonment from one to eight years. (3) Whoever without permission publishes or otherwise presents in public the essence of another's patent that has been applied for, before such patent is published in the manner set out by law, shall be punished with a fine or imprisonment up to two years. (4) Whoever without permission applies for a patent or fails to give or gives incorrect name of inventor in the application, shall be punished with imprisonment from six months to five years. (5) The things referred to in paragraphs 1 and 2 shall be seized and destroyed. **Criminal Code Art. 202 – Unauthorised Use of another's Design** (1) Whoever on his product in circulation uses without authorisation another's design which has been applied for or protected, shall be punished with a fine or imprisonment up to three years. (2) Whoever without authorisation publishes or otherwise presents in public the essence of another's design before it has been published in the manner set out by law, shall be punished with a fine or imprisonment up to one year. (3) The products referred to in paragraph 1 of this Article shall be seized.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 11 – Attempt and aiding or abetting 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.	**Criminal Code Art. 30 – Attempt** (1) Whoever commences a criminal offence with premeditation, but does not complete it, shall be punished for the attempted criminal offence if such offence is punishable by law with a term of imprisonment of five years or more, and for the attempt of other criminal offence only when the law explicitly provides for the punishment of attempt. (2) A perpetrator shall be punished for an attempt with a punishment prescribed for the criminal offence or with a lighter punishment. **Criminal Code Art. 34 – Incitement** (1) Whoever with intent incites another to commit a criminal offence shall be punished as prescribed by law for such offence. (2) Whoever with intent incites another to commit a criminal offence whose attempt is punishable by law, and such offence has not been attempted at all, shall be punished as for the attempted criminal offence. **Criminal Code Art. 35 – Aiding and Abetting** (1) Anyone aiding another with intent in committing a criminal offence shall be punished as prescribed by law for such criminal offence, or by a mitigated penalty. (2) The following, in particular, shall be considered as aiding in the commission of a criminal offence: giving instructions or advice on how to commit a criminal offence; supply of means for committing a criminal offence; creating conditions or removal of obstacles for committing a criminal offence; prior promise to conceal the commission of the offence, offender, means used in committing a criminal offence, traces of criminal offence and items gained through the commission of criminal offence.
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 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:	**Criminal Code Art. 12 – Liability of Legal Entities for Criminal Offences** Liability of legal entities for criminal offences as well as sanctions to be imposed on legal entities for criminal offences shall be regulated by a separate law

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**Law on the liability of legal entities for criminal offences Art.6. – The Grounds for Liability of Legal Entities** A legal person shall be held accountable for criminal offences which have been committed for the benefit of the legal person by a responsible person within the remit, that is, powers thereof. The liability referred to in paragraph 1 of this Article shall also exist where the lack of supervision or control by the responsible person allowed the commission of crime for the benefit of that legal person by a natural person operating under the supervision and control of the responsible person.
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.	
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:	**Criminal Procedure Code Art. 82 – Proving Facts in Proceedings** Evidence is collected and examined in proceedings in accordance with the provisions of this Code, and in other manner prescribed by law.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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.	**Criminal Procedure Code Art. 83 – Subject-matter of Evidentiary Actions** The subject-matter of evidentiary actions are the facts which constitute the elements of a criminal offence, or those on which application of another provision of criminal law depends. The subject-matter of evidentiary actions are also facts on which the application of provisions of criminal procedure depends. Facts assessed by the court as generally known, sufficiently examined, admitted to by the defendant in a manner making further examination of that evidence unnecessary (Article 88), or where the consent of the parties in relation to such facts is not contrary to other evidence, shall not be proven.
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	**Criminal Procedure Code Art. 3 – Presumption of Innocence** Everyone is considered innocent until proven guilty by a final decision of the court. Public and other authorities and organisations, the information media, associations and public figures are required to adhere to the rules referred to in paragraph 1 of this Article, as well as to abstain from violating the rights of the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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.	defendant with their public statements on the defendant, the criminal offence and the proceedings. **Criminal Procedure Code Art. 6 – Legality of Criminal Prosecution** The public prosecutor is required to conduct criminal prosecution where there are grounds for suspicion that a criminal offence has been committed or that a certain person has committed a criminal offence prosecutable ex officio. For certain criminal offences, where so prescribed by law, the public prosecutor may undertake criminal prosecution only on a motion by the injured party. By exception from paragraphs 1 and 2 of this Article, the public prosecutor may decide to defer criminal prosecution or not to undertake it, under conditions regulated by this Code. The public prosecutor and the police are required to impartially clear up suspicion about the criminal offence in connection with which they are conducting official activities, and to examine with equal attention both the facts against the defendant and the facts in his favour. **Criminal Procedure Code Art. 16 – Assessing Evidence and Finding of Fact** Court decisions may not be based on evidence which is, directly or indirectly, in itself or by the manner in which it was obtained, in contravention of the Constitution, this Code, other statute or universally accepted rules of international law and ratified international treaties, except in court proceedings in connection with the obtaining of such evidence. The court is required to make an impartial assessment of the evidence examined and based on the evidence to establish with equal care both the facts against the defendant and the facts which are in his favour. The court assesses the evidence examined which is of importance for rendering a decision at its discretion. The court may base its judgment, or ruling corresponding to a judgment, only on facts of whose certainty it is convinced. In case it has any doubts about the facts on which the conduct of criminal proceedings depends, the existence of the elements of a criminal offence, or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	application of another provision of criminal law, in its judgment, or ruling corresponding to a judgment, the court rules in favour of the defendant. **Criminal Procedure Code Art. 68 – The Defendant's Rights** The defendant is entitled: 1. to be informed in the shortest possible time, and always before the first interrogation, in detail and in a language, he understands, about the charges against him, the nature and grounds of the accusation, as well as that everything he says may be used as evidence in proceedings; 2. not to say anything, to refrain from answering a certain question, to present his defence freely, to admit or not to admit his culpability; 3. to defend himself on his own or with the professional assistance of a defence counsel, in accordance with the provisions of this Code; 4. to have a defence counsel attend his interrogation; 5. to be taken before a court in the shortest possible time and to be tried in an impartial and fair manner and in a reasonable time; 6. to read immediately before his first interrogation the criminal complaint, the crime scene report, and the findings and opinions of a expert witnesses; 7. to be given sufficient time and opportunity to prepare his defence; 8. to examine documents contained in the case file and objects serving as evidence; 9. to collect evidence for his own defence; 10. to state his position in relation to all the facts and evidence against him and to present facts and evidence in his favour, to question witnesses for the prosecution and to demand that witnesses for the defence be questioned in his presence, under the same conditions as the witnesses for the prosecution; 11. to make use of legal instruments and legal remedies; 12. to perform other actions where provided for by this Code. The authority conducting the proceedings is required to advise the defendant before his first interrogation of the rights referred to in paragraph 1, items s 2) to 4) and item 6) of this Article. **Criminal Procedure Code Art. 84 – Unlawful Evidence** Evidence collected in contravention of Article 16 paragraph 1 of this Code (unlawful evidence) may not be used in criminal proceedings.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Unlawful evidence is excluded from the case file, placed in a separate sealed cover and kept by the judge for preliminary proceedings until the final conclusion of the criminal proceedings, after which they are destroyed, and a record is made about their destruction. By exception from paragraph 2 of this Article, unlawful evidence is preserved until the final conclusion of court proceedings held in connection with the obtaining of such evidence. **Criminal Procedure Code Art. 161 – Requirements for Ordering** Special evidentiary actions may be ordered against a person for whom there are grounds for suspicion that he has committed a criminal offence referred to in Article 162 of this Code, and evidence for criminal prosecution cannot be acquired in another manner, or their gathering would be significantly hampered. Special evidentiary actions may also exceptionally be ordered against a person for whom there are grounds for suspicion that he is preparing one of the criminal offences referred to in paragraph 1 of this Article, and the circumstances of the case indicate that the criminal offence could not be detected, prevented or proved in another way, or that it would cause disproportionate difficulties or a substantial danger. In deciding on ordering and the duration of special evidentiary actions, the authority conducting proceedings will especially consider whether the same result could be achieved in a manner less restrictive to citizens' rights. **Criminal Procedure Code Art. 163 – Treatment of Collected Materials** If the public prosecutor does not initiate criminal proceedings within six months of the date of first examining the materials collected by applying special evidentiary actions or if he declares that he will not use them in the proceedings or that he will not request the conduct of proceedings against the suspect, the judge for preliminary proceedings will issue a ruling on the destruction of the collected materials. The judge for preliminary proceedings may inform the person against whom a special evidentiary action referred to in Article 166 of this Code was conducted about the issuance of the ruling referred to in paragraph 1 of this Article if during the conduct of the action his identity was established and if it would not threaten the possibility of conducting criminal proceedings. The materials are destroyed

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	under the supervision of the judge for preliminary proceedings who makes a record thereof. If during the performance of the special evidentiary actions it was acted in contravention of the provisions of this Code or an order of the authority conducting proceedings, the court's decision may not be based on the data collected and the collected material will be treated in accordance with Article 84 paragraph 3 of this Code. **Criminal Procedure Code Art. 237 – Excluding Transcripts and Information** When it is prescribed in this Code that certain evidence may not be used in criminal proceedings or that a court decision may not be based on it, the judge for preliminary proceedings will *ex officio* or on a motion of the parties and the defence counsel issue a ruling on excluding the transcript of those actions from the file immediately, or no later than the conclusion of the investigation. A special appeal against this ruling is allowed. After the ruling becomes final, the excluded transcripts are placed under a separate sealed cover and kept by the judge for preliminary proceedings separate from other documents and may not be examined or used in the proceedings. After the criminal proceedings are ended by a final decision, the excluded transcripts will be treated in accordance with Article 84 paragraph 2 and 3 of this Code. After the conclusion of the investigation, the judge for preliminary proceedings will act in accordance with provisions of paragraphs 1 and 2 of this Article also in respect of all information which was within the meaning of Article 282 paragraph 1 item 2) and paragraph 4 and Article 288 of this Code provided to the public prosecutor and police by citizens, except for the transcripts referred to in Article 289 paragraph 4 of this Code. When the public prosecutor files an indictment without conducting an investigation (Article 331 paragraph 5), he will deliver documentation with such information to the judge for preliminary proceedings, who will act in accordance with provisions of this Article. **Criminal Procedure Code Art. 358 – Excluding Unlawful Evidence** If the president of the panel determines that the casefile contains transcripts or information referred to in Article 237 paragraphs 1 and 3 of this Code, he will

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	issue a ruling on their exclusion from the files. A special appeal against this ruling is allowed. Upon the finality of the ruling referred to in paragraph 1 of this Article, the president of the panel will act in accordance with Article 237 paragraphs 2 and 3 of this Code. Until the conclusion of the evidentiary proceedings the panel may act in accordance with Article 407 paragraph 4 of this Code. **Criminal Procedure Code Art. 407 – Excluding Unlawful Evidence** The panel will issue a ruling ordering the following to be excluded from the files and kept separately: 1. transcripts of earlier examinations of persons which may not be read out for the reasons specified in Article 406 paragraph 2 of this Code; 2. the transcripts or information referred to in Article 237 paragraphs 1 and 3 of this Code. A special appeal is allowed against the ruling referred to in paragraph 1 of this Article. Upon the finality of the ruling referred to in paragraph 2 of this Article, the panel will act in accordance with Article 237 paragraphs 2 and 3 of this Code. If on the basis of examined evidence the panel finds that exclusion of evidence was not appropriate, it may until the conclusion of the evidentiary proceedings revoke the ruling referred to in paragraph 1 of this Article against which no appeal was filed and decide to examine the excluded evidence. **Criminal Procedure Code Art. 445 – Actions Taken by the Court of Second Instance with the Files** When the files reach the court of second instance in connection with an appeal, they are delivered to a reporting judge, and in particularly complex cases, several members of a panel may be reporting judges, which is decided upon by the president of the court. If a reporting judge determines that the files contain the transcripts or information referred to in Article 237 paragraphs 1 and 3 of this Code, he will issue a ruling excluding them from the files, against which a special appeal is

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	not allowed. After the ruling becomes final, the reporting judge will act in accordance with Article 237 paragraphs 2 and 3 of this Code. If a criminal offence prosecuted at the request of the public prosecutor is concerned, the reporting judge delivers the files to the competent public prosecutor, who is required to examine the files, make a motion and return them to the court without delay and not later than within 15 days, and in the case referred to in Article 432 paragraphs 2 and 3 of this Code, within 30 days. If the reporting judge determines that a judgment done in writing contains obvious errors, shortcomings or inconsistencies (Article 431), he will before the holding of a session of the second-instance panel return the files to the president of the first-instance panel to issue a ruling on rectifying the errors. After the ruling on rectifying the errors referred to in Article 431 paragraph 1 of this Code becomes final, the files will be delivered to the court of second instance, and in the case of a rectification of inconsistencies between a judgment done in writing and its original, it will be acted in accordance with Article 431 paragraph 2 of this Code.
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	Not covered.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 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.	Not covered.
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 held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:	**Criminal Procedure Code Art. 282 – Actions to be taken by the Public Prosecutor upon Receiving a Criminal Complaint** If the public prosecutor cannot assess from the criminal complaint if its assertions are probable, or if the data in the complaint do not provide sufficient grounds to decide whether to conduct an investigation, or if he finds out in some other way that a criminal offence has been committed, the public prosecutor may: 1. collect the necessary data himself; 2. request citizens [to provide information], under the conditions referred to in Article 288 paragraphs 1 to 6 of this Code; 3. submit a request to public and other authorities and legal persons to provide necessary information. A responsible person may be fined up to 150,000 dinars for failing to comply with the request of the public prosecutor referred to in paragraph 1 item 3) of this Article, and if after being fined he still refuses to provide the necessary

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	information, another fine in the same amount may be imposed on him once again. The decision on imposing the fine referred to in paragraph 2 of this Article is issued by the public prosecutor. An appeal against the ruling imposing the fine is decided by the judge for the preliminary proceedings. An appeal does not stay the execution of the ruling. If he is not able to undertake the actions referred to in paragraph 1 of this Article by himself, the public prosecutor will request the police to collect the necessary information and to undertake other measures and actions with the aim of uncovering the criminal offence and the perpetrator (Articles 286 to 288). The police are required to act in accordance with the request of the public prosecutor and to notify him about the measures and actions it had undertaken not later than 30 days from the date of receiving the request. In the case of a failure to act in accordance with the request, the public prosecutor will act in accordance with Article 44 paragraphs 2 and 3 of this Code. The public prosecutor, public and other authorities or legal persons are required during the collection of information or provision of data to act with due care and ensure that no damage is done to the honour and reputation of the person to whom the data relate.
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.	**Criminal Procedure Code Art. 147 – Objects Being Seized** The authority conducting proceedings will seize objects which must be seized under the Criminal Code or which may serve as evidence in criminal proceedings and secure their safekeeping. The decision on the seizure of funds which are the object of a suspicious transaction (Article 145) and their placement in a special account for safekeeping is issued by the court. Among the objects referred to in paragraph 1 of this Article are automatic data processing equipment and devices and equipment on which electronic records are kept or may be kept. **Criminal Procedure Code Art. 152 – Subject-matter and Grounds for a Search**

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 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. 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.	A search of a dwelling or other premise or a person may be performed if it is probable that the search will result in finding the defendant, traces of the criminal offence or objects of importance for the proceedings. A search of a dwelling or other premises or a person is performed on the basis of a court order or exceptionally without an order, on the basis of a legal authorisation. The search of automatic data processing devices and equipment on which electronic records are kept or may be kept is undertaken under a court order and, if necessary, with the assistance of an expert.
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	**Criminal Procedural Code - Special Evidentiary Actions - Requirements for Ordering - Article 161** Special evidentiary actions may be ordered against a person for whom there are grounds for suspicion that he has committed a criminal offence referred to in Article 162 of this Code, and evidence for criminal prosecution cannot be acquired in another manner, or their gathering would be significantly hampered. **Criminal Procedure Code Art. 166 – Conditions for Ordering** If the conditions referred to in Article 161 paragraphs 1 and 2 of this Code are fulfilled, acting on a reasoned request by the public prosecutor the court may order interception and recording of communications conducted by telephone or other technical means or surveillance of the electronic or other address of a suspect and the seizure of letters and other parcels. offences referred to in paragraph 1 of this Article, and the circumstances of the case indicate that the criminal offence could not be detected, prevented or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
communications transmitted 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.	proved in another way, or that it would cause disproportionate difficulties or a substantial danger.59 In deciding on ordering and the duration of special evidentiary actions, the authority conducting proceedings will especially consider whether the same result could be achieved in a manner less restrictive to citizens' rights. **Criminal Offences in Respect of Which Special Evidentiary Actions are Applied - Article 162** Under the conditions referred to in Article 161 of this Code, special evidentiary actions may be ordered for the following criminal offences: 1) those which according to separate statute fall within the competence of a prosecutor's office of special jurisdiction; 2) aggravated murder (Article 114 of the Criminal Code), abduction (Article 134 of the Criminal Code), showing, procurement and possession of pornographic materials and exploiting juveniles for pornography (Article 185 paragraphs 2 and 3 of the Criminal Code), extortion(Article 214 paragraph 4 of the Criminal Code), counterfeiting money (Article 223 paragraphs 1to 3 of the Criminal Code), money laundering (Article 231 paragraphs 1 to 4 of the Criminal Code), unlawful production and circulation of narcotic drugs (Article 246 paragraphs 1 to 3 of the Criminal Code), threatening independence (Article 305 of the Criminal Code), threatening territorial integrity (Article 307 of the Criminal Code), sedition (Article 308 of the Criminal Code), inciting sedition (Article 309 of the Criminal Code), subversion (Article 313 of the Criminal Code), sabotage (Article 314 of the Criminal Code), espionage (Article 315 of the Criminal Code), divulging state secrets (Article 316 of the Criminal Code), inciting national, racial and religious hatred or intolerance (Article 317 of the Criminal Code), violation of territorial sovereignty (Article 318 of the Criminal Code), conspiring to conduct activities against the Constitution (Article 319 of the Criminal Code), plotting an offences against the constitutional order and security of Serbia (Article 320 of the Criminal Code), serious offences against the constitutional order and security of Serbia (Article 321 of the Criminal Code), illegal manufacture, possession and sale of weapons and explosive materials (Article 348 paragraph 3 of the Criminal Code), illegal crossing of the national boarder and human trafficking (Article 350paragraphs 2 and 3 of the Criminal Code), abuse of office (Article 359 of the Criminal Code),trading in influences (Article 366 of the Criminal Code), taking

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	bribes (Article 367 of the Criminal Code), offering bribes (Article 368 of the Criminal Code), human trafficking (Article388 of the Criminal Code), taking hostages (Article 392 of the Criminal Code) and the criminal offence referred to in Article 98 paragraphs 3 to 5 of the Law on the Secrecy of Data; 3) obstruction of justice (Article 336 paragraph 1 of the Criminal Code), if committed in connection with the criminal offence referred to in items 1) and 2) of this paragraph. A special evidentiary action referred to in Article 183 of this Code may be ordered only in connection with a criminal offence referred to in paragraph 1 item 1) of this Article. Under the conditions referred to in Article 161 of this Code the special evidentiary action referred to in Article 166 of this Code may also be ordered for the following criminal offences: unauthorised exploitation of copyrighted work or other works protected by similar rights (Article199 of the Criminal Code), damaging computer data and programmes (Article 298 paragraph 3of the Criminal Code), computer sabotage (Article 299 of the Criminal Code), computer fraud(Article 301 paragraph 3 of the Criminal Code) and unauthorised access to protected computers, computer networks and electronic data processing (Article 302 of the Criminal Code). **Criminal Procedure Code Art. 167 – Order on Covert Interception of Communications** The special evidentiary action referred to in Article 166 of this Code is ordered by the judge for preliminary proceedings by a reasoned order. The order referred to in paragraph 1 of this Article contains available data on the person against whom the covert interception of communication is being ordered, legal designation of the criminal offence, designation of a known telephone number or address of the suspect or telephone number or address for which exist grounds for suspicion that the suspect is using, the reasons on which the suspicion is founded, manner of conduct, scope and duration of the special evidentiary action. Covert interception of communication may last three months, and if it is necessary in order to continue collecting evidence it may be extended by another three months at most. If criminal offences referred to in Article 162 paragraph 1 item 1) of this Code are concerned, covert interception may exceptionally be

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	extended at the most two times by another three months, respectively. The conduct of interception is discontinued as soon as the reasons for its application cease to exist. **Criminal Procedure Code Art. 168 – Conducting Covert Interception of Communications** The order referred to in Article 167 paragraph 1 of this Code is executed by the police, Security Information Agency or Military Security Agency. Daily reports are made on the conduct of the covert interception of communication and are together with the collected recordings of communications, letters or other parcels sent to the suspect or sent by the suspect, delivered to the judge for preliminary proceedings and the public prosecutor at their request. Postal, telegraphic and other enterprises, companies and persons registered for transmission of information are required to make accessible to the public authority referred to in paragraph 1 of this Article which executes the order the conduct of covert interception and recording of communications, and, with a receipt of delivery, hand over letters and other parcels.
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 legislative and other measures as may be necessary to ensure the real-time	**Criminal Procedural Code - Special Evidentiary Actions - Requirements for Ordering - Article 161** Special evidentiary actions may be ordered against a person for whom there are grounds for suspicion that he has committed a criminal offence referred to in Article 162 of this Code, and evidence for criminal prosecution cannot be acquired in another manner, or their gathering would be significantly hampered. **Criminal Procedure Code Art. 166 – Conditions for Ordering** If the conditions referred to in Article 161 paragraphs 1 and 2 of this Code are fulfilled, acting on a reasoned request by the public prosecutor the court may order interception and recording of communications conducted by telephone or other technical means or surveillance of the electronic or other address of a suspect and the seizure of letters and other parcels. offences referred to in paragraph 1 of this Article, and the circumstances of the case indicate that the criminal offence could not be detected, prevented or

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	proved in another way, or that it would cause disproportionate difficulties or a substantial danger.59 In deciding on ordering and the duration of special evidentiary actions, the authority conducting proceedings will especially consider whether the same result could be achieved in a manner less restrictive to citizens' rights. **Criminal Offences in Respect of Which Special Evidentiary Actions are Applied - Article 162** Under the conditions referred to in Article 161 of this Code, special evidentiary actions may be ordered for the following criminal offences: 1) those which according to separate statute fall within the competence of a prosecutor's office of special jurisdiction; 2) aggravated murder (Article 114 of the Criminal Code), abduction (Article 134 of the Criminal Code), showing, procurement and possession of pornographic materials and exploiting juveniles for pornography (Article 185 paragraphs 2 and 3 of the Criminal Code), extortion(Article 214 paragraph 4 of the Criminal Code), counterfeiting money (Article 223 paragraphs 1to 3 of the Criminal Code), money laundering (Article 231 paragraphs 1 to 4 of the Criminal Code), unlawful production and circulation of narcotic drugs (Article 246 paragraphs 1 to 3 of the Criminal Code), threatening independence (Article 305 of the Criminal Code), threatening territorial integrity (Article 307 of the Criminal Code), sedition (Article 308 of the Criminal Code), inciting sedition (Article 309 of the Criminal Code), subversion (Article 313 of the Criminal Code), sabotage (Article 314 of the Criminal Code), espionage (Article 315 of the Criminal Code), divulging state secrets (Article 316 of the Criminal Code), inciting national, racial and religious hatred or intolerance (Article 317 of the Criminal Code), violation of territorial sovereignty (Article 318 of the Criminal Code), conspiring to conduct activities against the Constitution (Article 319 of the Criminal Code), plotting an offences against the constitutional order and security of Serbia (Article 320 of the Criminal Code), serious offences against the constitutional order and security of Serbia (Article 321 of the Criminal Code), illegal manufacture, possession and sale of weapons and explosive materials (Article 348 paragraph 3 of the Criminal Code), illegal crossing of the national boarder and human trafficking (Article 350paragraphs 2 and 3 of the Criminal Code), abuse of office (Article 359 of the

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Criminal Code),trading in influences (Article 366 of the Criminal Code), taking bribes (Article 367 of the Criminal Code), offering bribes (Article 368 of the Criminal Code), human trafficking (Article388 of the Criminal Code), taking hostages (Article 392 of the Criminal Code) and the criminal offence referred to in Article 98 paragraphs 3 to 5 of the Law on the Secrecy of Data; 3) obstruction of justice (Article 336 paragraph 1 of the Criminal Code), if committed in connection with the criminal offence referred to in items 1) and 2) of this paragraph. A special evidentiary action referred to in Article 183 of this Code may be ordered only in connection with a criminal offence referred to in paragraph 1 item 1) of this Article. Under the conditions referred to in Article 161 of this Code the special evidentiary action referred to in Article 166 of this Code may also be ordered for the following criminal offences: unauthorised exploitation of copyrighted work or other works protected by similar rights (Article199 of the Criminal Code), damaging computer data and programmes (Article 298 paragraph 3of the Criminal Code), computer sabotage (Article 299 of the Criminal Code), computer fraud(Article 301 paragraph 3 of the Criminal Code) and unauthorised access to protected computers, computer networks and electronic data processing (Article 302 of the Criminal Code). **Criminal Procedure Code Art. 167 – Order on Covert Interception of Communications** The special evidentiary action referred to in Article 166 of this Code is ordered by the judge for preliminary proceedings by a reasoned order. The order referred to in paragraph 1 of this Article contains available data on the person against whom the covert interception of communication is being ordered, legal designation of the criminal offence, designation of a known telephone number or address of the suspect or telephone number or address for which exist grounds for suspicion that the suspect is using, the reasons on which the suspicion is founded, manner of conduct, scope and duration of the special evidentiary action.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Covert interception of communication may last three months, and if it is necessary in order to continue collecting evidence it may be extended by another three months at most. If criminal offences referred to in Article 162 paragraph 1 item 1) of this Code are concerned, covert interception may exceptionally be extended at the most two times by another three months, respectively. The conduct of interception is discontinued as soon as the reasons for its application cease to exist. **Criminal Procedure Code Art. 168 – Conducting Covert Interception of Communications** The order referred to in Article 167 paragraph 1 of this Code is executed by the police, Security Information Agency or Military Security Agency. Daily reports are made on the conduct of the covert interception of communication and are together with the collected recordings of communications, letters or other parcels sent to the suspect or sent by the suspect, delivered to the judge for preliminary proceedings and the public prosecutor at their request. *Postal, telegraphic and other enterprises, companies and persons registered for transmission of information are required to make accessible to the public authority referred to in paragraph 1 of this Article which executes the order the conduct of covert interception and recording of communications, and, with a receipt of delivery, hand over letters and other parcels.*
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 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.	**Criminal Code Art. 6 – Applicability of Criminal Legislation on the Territory of Serbia** (1) Criminal legislation of the Republic of Serbia shall apply to anyone committing a criminal offence on its territory. (2) Criminal legislation of the Republic of Serbia shall apply to anyone committing a criminal offence on a domestic vessel, regardless of where the vessel is at the time of committing of the act. (3) Criminal legislation of the Republic of Serbia shall apply to anyone committing a criminal offence in a domestic aircraft while in flight or domestic

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	military aircraft, regardless of where the aircraft is at the time of committing of criminal offence. (4) If criminal proceedings have been instituted or concluded in a foreign country in respect of cases specified in paragraphs 1 through 3 of this Article, criminal prosecution in Serbia shall be undertaken only with the permission of the Republic Public Prosecutor. (5) Criminal prosecution of foreign citizens in cases specified in paragraphs 1 through 3 of this Article may be transferred to a foreign state, under the terms of reciprocity.
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. 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	**Law on Mutual Assistance in criminal matters Articles 13 – 37.**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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.	**Law on Mutual Assistance in criminal matters Article 7 - Preconditions to the execution of requests for mutual assistance** Preconditions to the execution of requests for mutual assistance include: (1)The criminal offence, in respect of which legal assistance is requested, constitutes the offence under the legislation of the Republic of Serbia;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(2)The proceedings on the same offence have not been fully completed before the national court, that is, a criminal sanction has not been fully executed; (3) the criminal prosecution, that is, the execution of a criminal sanction is not excluded due to the state of limitations, amnesty or an ordinary pardon; (4) the request for legal assistance does not refer to a political offence or an offence relating to a political offence, that is, a criminal offence comprising solely violation of military duties; (5) the execution of requests for mutual assistance would not infringe sovereignty, security, public order or other interests of essential significance for the Republic of Serbia. Without prejudice to paragraph 1, sub-paragraph 4 of this Article, mutual assistance shall be granted for the criminal offence against the international humanitarian law that is not subject to the state of limitations. The competent judicial authority shall decide whether or not the preconditions under sub-paragraphs 1-3 of paragraph 1 have been met, whereas Minister of Justice shall decide or provide an opinion on whether or not the preconditions under sub-paragraphs 4 and 5 of paragraph 1 have been fulfilled. **Article 8 - Reciprocity** National judicial authorities shall grant mutual assistance subject to the rule of reciprocity. The Ministry of Justice shall provide a notification on the existence of reciprocity upon request of the national judicial authority. Should there be no information on reciprocity, the rule of reciprocity is presumed to exist.
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.	**Law on Mutual Assistance in criminal matters Art. 98 – Provision of information without the letter rogatory** Under the condition of reciprocity, national judicial authorities may transmit, without letter rogatory, information relating to known criminal offences and perpetrators to the competent authorities of the requesting party if this is considered to be of use to criminal proceedings conducted abroad. Transmission of information from paragraph 1 of this Article shall be performed only if it does not hinder criminal proceedings conducted in the Republic f Serbia.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 national judicial authority may request from the competent authority of the requesting party that received the information from paragraph 1 of this Article to notify the national authority about the activities undertaken and decisions reached.
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times. 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party. 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:	The Law on Mutual Assistance in criminal matters shall govern mutual assistance in criminal matters in cases in which no ratified international treaty exists or certain subject matters are not regulated under it.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities. 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary. 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly. 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party. b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol). c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**Law on Mutual Assistance in criminal matters Art. 9 – Confidentiality of information** It is the duty of state authorities to safeguard confidentiality of information obtained during the execution of requests for mutual legal assistance. Personal data may be used solely in criminal or administrative proceedings in respect of which letters rogatory have been submitted.
Article 29 – Expedited preservation of stored computer data 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	**Law on Mutual Assistance in criminal matters Art. 83 – Subject of other forms of mutual assistance** Other forms of mutual assistance include:

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. conduct of procedural activities such as issuance of summonses and delivery of writs, interrogation of the accused, examination of witnesses and experts, crime scene investigation, search of premises and persons, temporary seizure of objects; 2. implementation of measures such as surveillance and tapping of telephone and other conversations or communication as well as photographing or videotaping of persons, controlled delivery, provision of simulated business services, conclusion of simulated legal business, engagement of under-cover investigators, automatic data processing; 3. exchange of information and delivery of writs and cases related to criminal proceeding pending at the requesting party, delivery of data without the letter rogatory, use of audio and video-conference calls, forming of joint investigative teams; 4. temporary surrender of a person in custody for the purpose of examination by the requesting party's competent body.

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.	**Law on Mutual Assistance in criminal matters Art. 83 – Subject of other forms of mutual assistance** Other forms of mutual assistance include: 1. conduct of procedural activities such as issuance of summonses and delivery of writs, interrogation of the accused, examination of witnesses and experts, crime scene investigation, search of premises and persons, temporary seizure of objects; 2. implementation of measures such as surveillance and tapping of telephone and other conversations or communication as well as photographing or videotaping of persons, controlled delivery, provision of simulated business services, conclusion of simulated legal business, engagement of under-cover investigators, automatic data processing; 3. exchange of information and delivery of writs and cases related to criminal proceeding pending at the requesting party, delivery of data without the letter rogatory, use of audio and video-conference calls, forming of joint investigative teams; 4. temporary surrender of a person in custody for the purpose of examination by the requesting party's competent body. **Electronic Communications Law Art. 127 - Lawful Interception of Electronic Communications** The operator shall enable lawful interception of electronic communications referred to in paragraph 1 of Article 126 of this Law.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Relevant state authority which conducts lawful interception shall keep records on intercepted electronic communications which in particular include certain documents stipulating legal foundation for interception, the date and time of interception, and keep these records as confidential, pursuant to the law governing the confidentiality of data. When the relevant state authority which conducts lawful interception of electronic communications is not capable of conducting lawful interception of electronic communications without access to the premises, electronic communications network, associated facilities or electronic communications equipment of the operator, the operator from paragraph 1 of this Article shall keep records of the received requests for interception of electronic communications, which shall in particular include identification of the authorised person in charge of interception, the date and time of the interception, and keep these records as confidential, in accordance with the law which regulates the confidentiality of data. Pursuant to the provisions stipulated herein, for the purpose of meeting the obligation from paragraph 1 of this Article, the operator shall, at its own expense, provide necessary technical and organizational conditions (devices and program support), and forward evidence to substantiate the abovementioned to the Agency. Upon obtaining the opinions of the ministry in charge of judiciary affairs, the ministry in charge of internal affairs, the ministry in charge of defence affairs, Security and Information Agency and the authority in charge of the personal data protection, the Ministry shall prescribe in detail the requirements for devices and program support from paragraph 4 of this Article. **Electronic Communications Law Art. 128 - The Obligation of Data Retention** The operator shall retain data on electronic communications from paragraph 1 of Article 129 of this Law (hereinafter: retained data) for the purpose of conducting investigations, crime detection and criminal proceedings, in accordance with the law which regulates criminal proceedings, as well as for the purpose of protecting national and public security of the Republic of Serbia, according to the law which governs the operation of security services of the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Republic of Serbia and the operation of the authorities in charge of internal affairs. The operator from paragraph 1 of this Article shall retain the data in their authentic form or as data processed in the course of electronic communications activities. The operator from paragraph 1 of this Article need not retain data not produced or processed by it. The operator from paragraph 1 shall keep the retained data for 12 months after the communication has taken place. The operator shall retain data in such a manner that they can be accessed without delay, that they can be provided at request of the relevant state authority without delay, pursuant to paragraph 1 of this Article. The relevant state authority which accesses and/or which the retained data are provided for, shall keep records on the access and/or provided retained data that shall include in particular: reference to the document stipulating the legal foundation for access, and/or provision of retained data, date and time of access, and/or provision of retained data, and also keep these records as confidential, pursuant to the law which governs data confidentiality. When the relevant state authority is unable to access retained data without access to the premises, electronic communications network, associated facilities or electronic communications equipment of the operator, the operator from paragraph 1 of this Article shall keep records of the received requests for access and/or provision of retained data, which shall include in particular the identification of the authorised person who has accessed the retained data and/or who the retained data were provided to, reference to the document stipulating legal foundation for access and/or provision of retained data, as well as to keep these records as confidential, in accordance with the law which governs data confidentiality.
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	**Law on Mutual Assistance in criminal matters Art. 83 – Subject of other forms of mutual assistance** Other forms of mutual assistance include: 1. conduct of procedural activities such as issuance of summonses and delivery of writs, interrogation of the accused, examination of witnesses and

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where: a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	experts, crime scene investigation, search of premises and persons, temporary seizure of objects; 2. implementation of measures such as surveillance and tapping of telephone and other conversations or communication as well as photographing or videotaping of persons, controlled delivery, provision of simulated business services, conclusion of simulated legal business, engagement of under-cover investigators, automatic data processing; 3. exchange of information and delivery of writs and cases related to criminal proceeding pending at the requesting party, delivery of data without the letter rogatory, use of audio and video-conference calls, forming of joint investigative teams; 4. temporary surrender of a person in custody for the purpose of examination by the requesting party's competent body.
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.	Direct implementation of Convention.
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.	**Law on Mutual Assistance in criminal matters Art. 83 – Subject of other forms of mutual assistance** Other forms of mutual assistance include: 1. conduct of procedural activities such as issuance of summonses and delivery of writs, interrogation of the accused, examination of witnesses and experts, crime scene investigation, search of premises and persons, temporary seizure of objects; 2. implementation of measures such as surveillance and tapping of telephone and other conversations or communication as well as photographing or videotaping of persons, controlled delivery, provision of simulated business

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	services, conclusion of simulated legal business, engagement of under-cover investigators, automatic data processing; 3. exchange of information and delivery of writs and cases related to criminal proceeding pending at the requesting party, delivery of data without the letter rogatory, use of audio and video-conference calls, forming of joint investigative teams; 4. temporary surrender of a person in custody for the purpose of examination by the requesting party's competent body. **Criminal Procedural Code - Special Evidentiary Actions - Requirements for Ordering - Article 161** Special evidentiary actions may be ordered against a person for whom there are grounds for suspicion that he has committed a criminal offence referred to in Article 162 of this Code, and evidence for criminal prosecution cannot be acquired in another manner, or their gathering would be significantly hampered. Special evidentiary actions may also exceptionally be ordered against a person for whom there are grounds for suspicion that he is preparing one of the criminal offences referred to in paragraph 1 of this Article, and the circumstances of the case indicate that the criminal offence could not be detected, prevented or proved in another way, or that it would cause disproportionate difficulties or a substantial danger.59 In deciding on ordering and the duration of special evidentiary actions, the authority conducting proceedings will especially consider whether the same result could be achieved in a manner less restrictive to citizens' rights. **Criminal Offences in Respect of Which Special Evidentiary Actions are Applied - Article 162** Under the conditions referred to in Article 161 of this Code, special evidentiary actions may be ordered for the following criminal offences:1) those which according to separate statute fall within the competence of a prosecutor's office of special jurisdiction; 2) aggravated murder (Article 114 of the Criminal Code), abduction (Article 134 of the Criminal Code), showing, procurement and possession of pornographic

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	materials and exploiting juveniles for pornography (Article 185 paragraphs 2 and 3 of the Criminal Code), extortion(Article 214 paragraph 4 of the Criminal Code), counterfeiting money (Article 223 paragraphs 1to 3 of the Criminal Code), money laundering (Article 231 paragraphs 1 to 4 of the Criminal Code), unlawful production and circulation of narcotic drugs (Article 246 paragraphs 1 to 3 of the Criminal Code), threatening independence (Article 305 of the Criminal Code), threatening territorial integrity (Article 307 of the Criminal Code), sedition (Article 308 of the Criminal Code), inciting sedition (Article 309 of the Criminal Code), subversion (Article 313 of the Criminal Code), sabotage (Article 314 of the Criminal Code), espionage (Article 315 of the Criminal Code), divulging state secrets (Article 316 of the Criminal Code), inciting national, racial and religious hatred or intolerance (Article 317 of the Criminal Code), violation of territorial sovereignty (Article 318 of the Criminal Code), conspiring to conduct activities against the Constitution (Article 319 of the Criminal Code), plotting an offences against the constitutional order and security of Serbia (Article 320 of the Criminal Code), serious offences against the constitutional order and security of Serbia (Article 321 of the Criminal Code), illegal manufacture, possession and sale of weapons and explosive materials (Article 348 paragraph 3 of the Criminal Code), illegal crossing of the national boarder and human trafficking (Article 350paragraphs 2 and 3 of the Criminal Code), abuse of office (Article 359 of the Criminal Code),trading in influences (Article 366 of the Criminal Code), taking bribes (Article 367 of the Criminal Code), offering bribes (Article 368 of the Criminal Code), human trafficking (Article388 of the Criminal Code), taking hostages (Article 392 of the Criminal Code) and the criminal offence referred to in Article 98 paragraphs 3 to 5 of the Law on the Secrecy of Data; 3) obstruction of justice (Article 336 paragraph 1 of the Criminal Code), if committed in connection with the criminal offence referred to in items 1) and 2) of this paragraph. A special evidentiary action referred to in Article 183 of this Code may be ordered only in connection with a criminal offence referred to in paragraph 1 item 1) of this Article. Under the conditions referred to in Article 161 of this Code the special evidentiary action referred to in Article 166 of this Code may also be ordered for the following criminal offences: unauthorised exploitation of copyrighted work or other works protected by similar rights (Article199 of the Criminal Code), damaging computer data and programmes (Article 298 paragraph 3of the Criminal Code), computer

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	sabotage (Article 299 of the Criminal Code), computer fraud(Article 301 paragraph 3 of the Criminal Code) and unauthorised access to protected computers, computer networks and electronic data processing (Article 302 of the Criminal Code).
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.	**Law on Mutual Assistance in criminal matters Art. 83 – Subject of other forms of mutual assistance** Other forms of mutual assistance include: 1. conduct of procedural activities such as issuance of summonses and delivery of writs, interrogation of the accused, examination of witnesses and experts, crime scene investigation, search of premises and persons, temporary seizure of objects; 2. implementation of measures such as surveillance and tapping of telephone and other conversations or communication as well as photographing or videotaping of persons, controlled delivery, provision of simulated business services, conclusion of simulated legal business, engagement of under-cover investigators, automatic data processing; 3. exchange of information and delivery of writs and cases related to criminal proceeding pending at the requesting party, delivery of data without the letter rogatory, use of audio and video-conference calls, forming of joint investigative teams; 4. temporary surrender of a person in custody for the purpose of examination by the requesting party's competent body. **Criminal Procedural Code - Special Evidentiary Actions - Requirements for Ordering - Article 161** Special evidentiary actions may be ordered against a person for whom there are grounds for suspicion that he has committed a criminal offence referred to in Article 162 of this Code, and evidence for criminal prosecution cannot be acquired in another manner, or their gathering would be significantly hampered. Special evidentiary actions may also exceptionally be ordered against a person for whom there are grounds for suspicion that he is preparing one of the criminal offences referred to in paragraph 1 of this Article, and the circumstances of the case indicate that the criminal offence could not be detected, prevented or

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	proved in another way, or that it would cause disproportionate difficulties or a substantial danger.59 In deciding on ordering and the duration of special evidentiary actions, the authority conducting proceedings will especially consider whether the same result could be achieved in a manner less restrictive to citizens' rights. **Criminal Offences in Respect of Which Special Evidentiary Actions are Applied - Article 162** Under the conditions referred to in Article 161 of this Code, special evidentiary actions may be ordered for the following criminal offences:1) those which according to separate statute fall within the competence of a prosecutor's office of special jurisdiction; 2) aggravated murder (Article 114 of the Criminal Code), abduction (Article 134 of the Criminal Code), showing, procurement and possession of pornographic materials and exploiting juveniles for pornography (Article 185 paragraphs 2 and 3 of the Criminal Code), extortion(Article 214 paragraph 4 of the Criminal Code), counterfeiting money (Article 223 paragraphs 1to 3 of the Criminal Code), money laundering (Article 231 paragraphs 1 to 4 of the Criminal Code), unlawful production and circulation of narcotic drugs (Article 246 paragraphs 1 to 3 of the Criminal Code), threatening independence (Article 305 of the Criminal Code), threatening territorial integrity (Article 307 of the Criminal Code), sedition (Article 308 of the Criminal Code), inciting sedition (Article 309 of the Criminal Code), subversion (Article 313 of the Criminal Code), sabotage (Article 314 of the Criminal Code), espionage (Article 315 of the Criminal Code), divulging state secrets (Article 316 of the Criminal Code), inciting national, racial and religious hatred or intolerance (Article 317 of the Criminal Code), violation of territorial sovereignty (Article 318 of the Criminal Code), conspiring to conduct activities against the Constitution (Article 319 of the Criminal Code), plotting an offences against the constitutional order and security of Serbia (Article 320 of the Criminal Code), serious offences against the constitutional order and security of Serbia (Article 321 of the Criminal Code), illegal manufacture, possession and sale of weapons and explosive materials (Article 348 paragraph 3 of the Criminal Code), illegal crossing of the national boarder and human trafficking (Article 350paragraphs 2 and 3 of the Criminal Code), abuse of office (Article 359 of the Criminal Code),trading in influences (Article 366 of the Criminal Code), taking

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	bribes (Article 367 of the Criminal Code), offering bribes (Article 368 of the Criminal Code), human trafficking (Article388 of the Criminal Code), taking hostages (Article 392 of the Criminal Code) and the criminal offence referred to in Article 98 paragraphs 3 to 5 of the Law on the Secrecy of Data; 3) obstruction of justice (Article 336 paragraph 1 of the Criminal Code), if committed in connection with the criminal offence referred to in items 1) and 2) of this paragraph. A special evidentiary action referred to in Article 183 of this Code may be ordered only in connection with a criminal offence referred to in paragraph 1 item 1) of this Article. Under the conditions referred to in Article 161 of this Code the special evidentiary action referred to in Article 166 of this Code may also be ordered for the following criminal offences: unauthorised exploitation of copyrighted work or other works protected by similar rights (Article199 of the Criminal Code), damaging computer data and programmes (Article 298 paragraph 3of the Criminal Code), computer sabotage (Article 299 of the Criminal Code), computer fraud(Article 301 paragraph 3 of the Criminal Code) and unauthorised access to protected computers, computer networks and electronic data processing (Article 302 of the Criminal Code).
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.	In compliance with Article 35 of the Budapest Convention, 24/7 point of contact was established in the Department for Fight Against High-Tech Crime of the Ministry of Interior and the Special Prosecution Office for High-Tech Crime.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
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.	**Declaration contained in a letter from the Chargée d'affaires a.i. of Serbia, dated 16 July 2009, registered at the Secretariat General on 16 July 2009 – Or. Engl.** In accordance with Articles 24, 27 and 35 of the Convention, Serbia designates as the central authorities in charge for the implementation of the Convention: Ministry of Interior of the Republic of Serbia Directorate of Crime Police Department for the fight against organized crime

Back to the Table of Contents