Project on Cybercrime
www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Version 30 May 2007
[Reformat in February 2011]

Cybercrime legislation – country profile

SLOVAK REPUBLIC

This profile has been prepared within the framework of the Council of Europe's capacity building projects on cybercrime in view of sharing information and assessing the current state of implementation of the Convention on Cybercrime under domestic legislation. It does not necessarily reflect official positions of the country covered or of the Council of Europe.

Comments may be sent to:

Economic Crime Division
Directorate General of Human Rights and Legal Affairs
Council of Europe, Strasbourg, France

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

Country:	**Slovak Republic**
Signature of Convention:	04.02.2005
Ratification/accession:	No
Provisions of the Convention	***Corresponding provisions/solutions in national legislation*** *(pls quote or summarise briefly; pls attach relevant extracts as an appendix)*
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	**SEC. 247 of the Criminal Code Act no 300/2005 Coll., Damaging and misusing a record in the information carrier** (1) Any one shall be liable to a sentence of deprivation of liberty for six months up to three years, who obtains/gains unauthorized access to a computer

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	system or to other information carrier or to a part of it with the intent to cause a damage or any other prejudice to another, or to obtain undue advantage for himself or for another and who a) shall make unauthorized use of an information contained there b) destroys, damages, deletes, alters or reduces/worsens a quality of an information in it c) interferes with the technical or program equipment of a computer, or d) enters, transfers/transmits, damages, deletes, reduces quality, alters or restraints/suppresses the computer data in order to obstruct/hinder the functionality/operation of a computer system, or who creates unauthentic data with the intent such data are deemed authentic or used so for legal purposes. (2) The same sentence as referred to in the par. 1 shall be imposed to any one who for the purpose of a criminal offence described in the par. 1 a) without authorization and by means of technical devices shall watch/monitor a non public/close transfer of computer data into a computer system, from it or within it, or b) procures/obtains or makes access to a computer program or other devices, to a computer password, access code or any similar data permitting/enabling access to whole/entire computer system or to its part.
Chapter II – Measures to be taken at the national level ***Section 1 – Substantive criminal law***	
Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems	
Article 2 – Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected	**SEC. 247 (1) of the Criminal Code Act no 300/2005 Coll.** (1) Any one shall be liable to a sentence of deprivation of liberty for six months up to three years, who obtains/gains unauthorized access to a computer system or to other information carrier or to a part of it with the intent to cause a damage or any other prejudice to another, or to obtain undue advantage for himself or for another and who

to another computer system.	a) shall make unauthorized use of an information contained there b) destroys, damages, deletes, alters or reduces/worsens a quality of an information in it c) interferes with the technical or program equipment of a computer, or d) enters, transfers/transmits, damages, deletes, reduces quality, alters or restraints/suppresses the computer data in order to obstruct/hinder the functionality/operation of a computer system, or who creates unauthentic data with the intent such data are deemed authentic or used so for legal purposes.
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.	**SEC. 247 (2) a of the Criminal Code Act no 300/2005 Coll.** (1) The same sentence as referred to in the par. 1 shall be imposed to any one who for the purpose of a criminal offence described in the par. 1 a) without authorization and by means of technical devices shall watch/monitor a non public/close transfer of computer data into a computer system, from it or within it, or b) procures/obtains or makes access to a computer program or other devices, to a computer password, access code or any similar data permitting/enabling access to whole/entire computer system or to its part.
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.	**SEC. 247 (1) b, d of the Criminal Code Act no 300/2005 Coll.** (1)The same sentence as referred to in the par. 1 shall be imposed to any one who for the purpose of a criminal offence described in the par. 1 b)procures/obtains or makes access to a computer program or other devices, to a computer password, access code or any similar data permitting/enabling access to whole/entire computer system or to its part. d)enters, transfers/transmits, damages, deletes, reduces quality, alters or restraints/suppresses the computer data in order to obstruct/hinder the functionality/operation of a computer system, or who creates unauthentic data with the intent such data are deemed

	authentic or used so for legal purposes
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	**SEC. 247 (1) d of the Criminal Code Act no 300/2005 Coll.** (1)The same sentence as referred to in the par. 1 shall be imposed to any one who for the purpose of a criminal offence described in the par. 1 d)enters, transfers/transmits, damages, deletes, reduces quality, alters or restraints/suppresses the computer data in order to obstruct/hinder the functionality/operation of a computer system, or who creates unauthentic data with the intent such data are deemed authentic or used so for legal purposes
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, 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,	**SEC. 247 (1) c of the Criminal Code Act no 300/2005 Coll.** (1)The same sentence as referred to in the par. 1 shall be imposed to any one who for the purpose of a criminal offence described in the par. 1 c)interferes with the technical or program equipment of a computer, or

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.	
Title 2 – Computer-related offences	
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, 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.	**SEC. 247 (1) d of the Criminal Code Act no 300/2005 Coll.** (1)The same sentence as referred to in the par. 1 shall be imposed to any one who for the purpose of a criminal offence described in the par. 1 d)enters, transfers/transmits, damages, deletes, reduces quality, alters or restraints/suppresses the computer data in order to obstruct/hinder the functionality/operation of a computer system, or who creates unauthentic data with the intent such data are deemed authentic or used so for legal purposes
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.	**SEC. 226 of the Criminal Code Act no 300/2005 Coll.** **Undue enrichment** (1) Any one shall be liable to a sentence of deprivation of liberty up to two years who by means of unauthorized interference with the technical or program equipment of a computer, automate, or any other similar device serving for automatic sale of goods, exchange or withdrawal of money or for providing automatic and paid performance, services, or for any other performance obtains/acquires goods, services or information without required payment or who obtains a money illegally and enriches himself or another to a prejudice of another person's property causing a small damage to another persons' property.
Title 3 – Content-related offences	
Article 9 – Offences related to child pornography 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a	**SEC. 368-370 of the Criminal Code Act no 300/2005 Coll.** **Section 368 Production/manufacturing child pornography** (1) Any one shall be liable to a sentence of deprivation of liberty for four up to ten years who makes use, offers or otherwise abuses a child for the purpose of producing child pornography or who permits/allows for such abuse or

computer system; 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.	who participates in such production any other manner. **Section 369 Distribution of child pornography** (1) Any one shall be liable to a sentence of deprivation of liberty for one up to five years who reproduces, transports, procures, makes access to or otherwise distributes child pornography. **Section 370 Sheltering/storing child pornography** Any one shall be liable to a sentence of deprivation of liberty for up to two years who stores/conceals child pornography.
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the	**SEC. 283 of the Criminal Code Act no 300/2005 Coll., Breach of copyright** Any one shall be liable to a sentence of deprivation of liberty for maximum term of two years who unlawfully interferes with the legally protected rights to a work, artistic performance, audio record or audio and video record, broadcasting or televising or to a database.

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.	
Title 5 – Ancillary liability and sanctions	
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.	**SEC. 14 (1), 20, 21(1)d of the Criminal Code Act no 300/2005 Coll.** **Section 14 Attempted crime** (1) Attempted crime means an acting which directly aims to completing a commission of a criminal offence and which was committed by a perpetrator if a criminal offence was not completed. (2) Attempted crime is punishable according to a severity of sentence imposed for completed criminal offence. **Section 20 Accomplice** If a criminal offence was committed by joint acting of two or more perpetrators (accomplices), each one of them is accountable for it like he/she would have committed it alone. **Section 21 Participant in a crime (accessory)** (1) A person is considered/deemed a participant in a completed or

	attempted crime if he/she intentionally plotted or directed commission of a crime (organizer) counseled another to commit a crime (abettor) requested another to commit a crime (orderer), or assisted another in committing a crime, in particular by procuring means, removing obstacles, counseling/advising, strengthening resolution, promising assistance in committing a crime (aider, assisting offender). (2) Provisions about criminal responsibility of a perpetrator shall apply to the criminal responsibility of a participant in a crime unless provided otherwise in this Act. *note no 1:* The Slovak Republic has not implemented the criminal responsibility of legal entities in its criminal codes so far. Nowadays, legal entities may be sanctioned only within the scope of administrative law.
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: 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.	The Slovak Republic has not implemented the criminal responsibility of legal entities in its criminal codes so far. Nowadays, legal entities may be sanctioned only within the scope of administrative law.

4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	
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.	**For the art 13(1) of Convention on Cybercrime - SEC. 196,247,369,283 of the Criminal Code Act no 300/2005 Coll.** **SEC. 247 of the Criminal Code Act no 300/2005 Coll., Damaging and misusing a record in the information carrier** (3) Any one shall be liable to a sentence of deprivation of liberty for six months up to three years, who obtains/gains unauthorized access to a computer system or to other information carrier or to a part of it with the intent to cause a damage or any other prejudice to another, or to obtain undue advantage for himself or for another and who a) shall make unauthorized use of an information contained there b) destroys, damages, deletes, alters or reduces/worsens a quality of an information in it c) interferes with the technical or program equipment of a computer, or d) enters, transfers/transmits, damages, deletes, reduces quality, alters or restraints/suppresses the computer data in order to obstruct/hinder the functionality/operation of a computer system, or who creates unauthentic data with the

	intent such data are deemed authentic or used so for legal purposes. (4) The same sentence as referred to in the par. 1 shall be imposed to any one who for the purpose of a criminal offence described in the par. 1 a) without authorization and by means of technical devices shall watch/monitor a non public/close transfer of computer data into a computer system, from it or within it, or b) procures/obtains or makes access to a computer program or other devices, to a computer password, access code or any similar data permitting/enabling access to whole/entire computer system or to its part. **Section 369** - **Distribution of child pornography** (1) Any one shall be liable to a sentence of deprivation of liberty for one up to five years who reproduces, transports, procures, makes access to or otherwise distributes child pornography. **Section 283 - Breach of copyright** (1) Any one shall be liable to a sentence of deprivation of liberty for maximum term of two years who unlawfully interferes with the legally protected rights to a work, artistic performance, audio record or audio and video record, broadcasting or televising or to a database.
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2	**SEC. 90,118 of the Code of Criminal Procedure Act no 301/2005 Coll.** **Section 90 - Storing and delivering (handing over) of computer data** (1) If storage of saved computer data including traffic data saved by means of computer system is necessary in order to clarify facts significant for criminal proceedings, then presiding judge or a prosecutor within pre-trial proceedings or prior to the commencement of criminal prosecution may issue an

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	order that needs to be justified by factual circumstances and addressed to a person in whose possession or under whose control such data are, or to a service provider of such services, with the view of: a) storing and keeping completeness of such data b) enabling production and keeping/possession of copies of such data c) making access to such data impossible d) removing from computer system such data e) handing over such data for the purposes of criminal proceedings. (2) The order issued pursuant to the par. 1 must state a period of time during which data storage shall be carried out, maximum period is 90 days, and if repeated storage is necessary, new order shall be issued. (3) If storage is no longer necessary of computer data including traffic data for the purposes of criminal proceedings, presiding judge or prosecutor in the stage before the commencement of criminal prosecution or within pre-trial proceedings shall issue the order to cancel data storage without delay. (4) An order issued pursuant to the par. 1 to 3 shall be served on a person in whose possession or control the data are or to a service provider of such services; both of them may be imposed the obligation of keeping in secret the measures contained in the order. **Section 118 - Comparison of data found in different computer systems** (1) Comparison of data within different information systems containing characteristic/typical or excluding features of persons or things material for criminal proceedings may be carried out if necessary for clarification of a crime within criminal proceedings on willful criminal act liable to a sentence of deprivation of liberty with the maximum term exceeding 3 years, on corruption or on any other willful crime if such proceedings are to be conducted pursuant to a binding international treaty. (2) Written order to compare data in different information systems shall be issued by presiding judge or by prosecutor within proceedings prior to commencement of criminal prosecution or within pre-trial proceedings.

	(3) An order issued pursuant to the par 1 shall contain name of information system operator who is obliged to hand over the data as well as definition of data and also testing data that are necessary for comparison. (4) A person defined in the par. 3 is obliged to provide data necessary for the comparison. If the data requested are inseparable from other data, then other data shall be handed over as well. Such other data may not be used as evidence. (5) If data were provided in an information carrier, they shall be returned back immediately after termination of a comparison. Data transferred to other information carriers shall be immediately destroyed by that law enforcement officer/court/police officer who carried out the comparison, if such data are not longer necessary for criminal proceedings. (6) If a record made from data comparison is to be used as evidence, the procedure shall be carried out pursuant to the Section 115 accordingly. (7) Record may be used as evidence in another criminal matter different from that one within which a comparison had been made only if there is simultaneous criminal proceedings conducted in that matter concerning some of the criminal acts as referred to in the par. 1. (8) If no material facts are found for criminal proceedings as result of comparison, then that law enforcement authority/court/police which had carried out the comparison, shall immediately destroy the record obtained and he shall do it in prescribed manner.
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	**SEC.14-25 of SK Constitution, SEC. 90,118 of the Code of Criminal Procedure Act no 301/2005 Coll.** **Section 90 - Storing and delivering (handing over) of computer data** (1) If storage of saved computer data including traffic data saved by means of computer system is necessary in order to clarify facts significant for

Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. 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.	criminal proceedings, then presiding judge or a prosecutor within pre-trial proceedings or prior to the commencement of criminal prosecution may issue an order that needs to be justified by factual circumstances and addressed to a person in whose possession or under whose control such data are, or to a service provider of such services, with the view of: a) storing and keeping completeness of such data b) enabling production and keeping/possession of copies of such data c) making access to such data impossible d) removing from computer system such data e) handing over such data for the purposes of criminal proceedings. (2) The order issued pursuant to the par. 1 must state a period of time during which data storage shall be carried out, maximum period is 90 days, and if repeated storage is necessary, new order shall be issued. (3) If storage is no longer necessary of computer data including traffic data for the purposes of criminal proceedings, presiding judge or prosecutor in the stage before the commencement of criminal prosecution or within pre-trial proceedings shall issue the order to cancel data storage without delay. (4) An order issued pursuant to the par. 1 to 3 shall be served on a person in whose possession or control the data are or to a service provider of such services; both of them may be imposed the obligation of keeping in secret the measures contained in the order. **Section 118 - Comparison of data found in different computer systems** (1) Comparison of data within different information systems containing characteristic/typical or excluding features of persons or things material for criminal proceedings may be carried out if necessary for clarification of a crime within criminal proceedings on willful criminal act liable to a sentence of deprivation of liberty with the maximum term exceeding 3 years, on corruption or on any other willful crime if such proceedings are to be conducted pursuant to a binding international treaty. (2) Written order to compare data in different information systems shall be

	issued by presiding judge or by prosecutor within proceedings prior to commencement of criminal prosecution or within pre-trial proceedings. (3) An order issued pursuant to the par 1 shall contain name of information system operator who is obliged to hand over the data as well as definition of data and also testing data that are necessary for comparison. (4) A person defined in the par. 3 is obliged to provide data necessary for the comparison. If the data requested are inseparable from other data, then other data shall be handed over as well. Such other data may not be used as evidence. (5) If data were provided in an information carrier, they shall be returned back immediately after termination of a comparison. Data transferred to other information carriers shall be immediately destroyed by that law enforcement officer/court/police officer who carried out the comparison, if such data are not longer necessary for criminal proceedings. (6) If a record made from data comparison is to be used as evidence, the procedure shall be carried out pursuant to the Section 115 accordingly. (7) Record may be used as evidence in another criminal matter different from that one within which a comparison had been made only if there is simultaneous criminal proceedings conducted in that matter concerning some of the criminal acts as referred to in the par. 1. (8) If no material facts are found for criminal proceedings as result of comparison, then that law enforcement authority/court/police which had carried out the comparison, shall immediately destroy the record obtained and he shall do it in prescribed manner.
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.	**SEC. 90 (1)a of the Code of Criminal Procedure Act no 301/2005 Coll.** (1) If storage of saved computer data including traffic data saved by means of computer system is necessary in order to clarify facts significant for criminal proceedings, then presiding judge or a prosecutor within pre-trial proceedings or prior to the commencement of criminal prosecution may issue an order that needs to be justified by factual circumstances

2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	and addressed to a person in whose possession or under whose control such data are, or to a service provider of such services, with the view of: a) storing and keeping completeness of such data
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.	**SEC. 90 (1)a, b, e of the Code of Criminal Procedure Act no 301/2005 Coll.** (1) If storage of saved computer data including traffic data saved by means of computer system is necessary in order to clarify facts significant for criminal proceedings, then presiding judge or a prosecutor within pre-trial proceedings or prior to the commencement of criminal prosecution may issue an order that needs to be justified by factual circumstances and addressed to a person in whose possession or under whose control such data are, or to a service provider of such services, with the view of: a)storing and keeping completeness of such data b)enabling production and keeping/possession of copies of such data e)handing over such data for the purposes of criminal proceedings.
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	**SEC. 90 (1)e, 118 (3) of the Code of Criminal Procedure Act no 301/2005 Coll.** **SEC. 90 (1) e of the Code of Criminal Procedure Act no 301/2005 Coll.**

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: 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.	(1) If storage of saved computer data including traffic data saved by means of computer system is necessary in order to clarify facts significant for criminal proceedings, then presiding judge or a prosecutor within pre-trial proceedings or prior to the commencement of criminal prosecution may issue an order that needs to be justified by factual circumstances and addressed to a person in whose possession or under whose control such data are, or to a service provider of such services, with the view of: e)handing over such data for the purposes of criminal proceedings. **Section 118 - Comparison of data found in different computer systems** (3)An order issued pursuant to the par 1 shall contain name of information system operator who is obliged to hand over the data as well as definition of data and also testing data that are necessary for comparison.
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.	**SEC. 91 of the Code of Criminal Procedure Act no 301/2005 Coll., Seizure of a thing** (1) If upon a demand a person fails to render a thing or computer data that are material for criminal proceedings, then - upon an order issued by a presiding judge or a by prosecutor within pre-trial proceedings or by a police officer – such thing may be seized to a person. Prior consent by a prosecutor is necessary for the police for issuing such order. (2) If the authority issuing the order to seize does not execute itself a seizure of a thing, the police shall execute it upon an order. (3) Police may issue an order without prior consent pursuant to the par. 1 only in the event where prior consent is impossible to be given and the matter is urgent. (4) If possible, the unparticipating person shall be involved in the

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.	seizure of a thing. (5) A person or service provider who is in possession/control of the computer data or of information about the services concerned shall hand over/deliver them to a person who had issued the order pursuant to the par. 1.
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	**SEC. 90 (1)a, b, e of the Code of Criminal Procedure Act no 301/2005 Col**l. (1) If storage of saved computer data including traffic data saved by means of computer system is necessary in order to clarify facts significant for criminal proceedings, then presiding judge or a prosecutor within pre-trial proceedings or prior to the commencement of criminal prosecution may issue an order that needs to be justified by factual circumstances and addressed to a person in whose possession or under whose control such data are, or to a service provider of such services, with the view of: a)storing and keeping completeness of such data b)enabling production and keeping/possession of copies of such data e)handing over such data for the purposes of criminal proceedings.

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.	
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 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.	
Section 3 – Jurisdiction	
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be	**SEC. 3 of the of the Criminal Code Act no 300/2005 Coll., Territorial competence/jurisdiction**

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. 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.	(1) Pursuant to this Act, the punishability of an act committed in the territory of the Slovak Republic shall be examined. (2) A criminal act is deemed/considered to be committed in the territory of the Slovak Republic even in the case where the offender a) committed the act partially in the SK territory, if breach or endangering of an interest protected by this Act has occurred or should/might occur either entirely or partially in the territory of the Slovak Republic, or b) committed an act outside SK territory if breach or endangering of an interest protected by this Act should occur here, or if such consequence might occur here even partially. (3) Pursuant to this Act, punishability of an act shall also be examined if committed outside SK territory on board of a ship flying the Slovak flag or on board of an aircraft recorded in the Aircraft Register of the Slovak Republic.
Chapter III – International co-operation	
Article 24 – Extradition 1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty	**SEC. 498-514 of the Code of Criminal Procedure Act no 301/2005 Coll.** In whole its extent, the SK domestic/internal regulation corresponds with the Article 24, Convention on Cybercrime. Within the extradition proceedings, the Slovak authorities proceed according to the provisions of the section 489 to 514, of the Code of Criminal Procedure of the Slovak Republic, as well as international treaties by which the Slovak Republic is bound and also pursuant to the rules of international law.

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 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	**SEC. 1(2) of the SK Constitution, SEC. 531-537 of the Code of Criminal**

1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35. 3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.	**Procedure Act no 301/2005 Coll.** **Section 537 Method and form of handling a request** (1) Slovak authorities shall execute a request made by foreign authorities in a manner stipulated by this Act or by an international treaty. If mutual assistance is made pursuant to an international treaty in a manner that is not regulated in this Act, then a competent prosecutor shall decide on a method of executing legal assistance. (2) Upon request by foreign authority, the requested legal assistance may be executed pursuant to the legal rule of requesting country unless the requested procedure is contrary to the interests protected by the provision of the Section 481. (3) In order to execute a request pursuant to the Section 539, par. 1, it is required that the act in relation to which the request is made, should be criminal act not only pursuant to the legal order of the requesting country, but also pursuant to the legal order of the Slovak Republic. Explanatory comments on the provision of the Section 537, Code of Criminal Procedure of the Slovak Republic (extract): *The mentioned provision explicitly expresses the basic principle of executing legal assistance pursuant to the law of the requested country (lex fori).* *It regulates the extent/scope of the legal assistance awarded so that it restricts/limits it by means of legal regulation of this Act or an international treaty. Upon request by foreign authorities, competent SK authorities may execute in principle any act they are competent to carry out within criminal proceedings conducted in the Slovak Republic or any act regulated by an international treaty. Extent of mutual assistance so defined is also limited by the following elements:*

	- *in absence of international treaty, actual reciprocity is a prerequisite of carrying out legal assistance i.e. competent authorities of the requesting country are expected to provide the same type of legal assistance as they are requesting for in a similar case,* - *execution of some specific legal assistance acts is conditioned by contractual reciprocity (Section 544, 551), the execution of them is excluded in absence of contractual regulation,* - *no significant protected SK interest shall be hindered through execution of requested acts (section 481).* *If requesting authority requests execution of an act pursuant to an international treaty by which SK is bound, whilst the requested method is not regulated in this Act, competent prosecutor shall decide on a manner/method of execution of legal assistance act (Section 538, par.2).* *If requesting authority requests for execution of an act on the basis of an international treaty containing regulation of specific procedure/method that is more detailed or different from domestic legal order regulation, then the act shall be executed pursuant to the international treaty and competent prosecutor shall decide on modalities of carrying out of the act (Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters).* *The provision of the par. 2 admits/allows execution of the legal assistance act pursuant to the legal order of a foreign country, unless such method is contrary to the important protected interests of the Slovak Republic (Section 481) that represents breaching of the basic principle lex fori.* *In such case, competent prosecutor is obliged to submit to the court a request for decision pursuant to the Section 539, par. 2. Court shall decide on existence, absence of conflict with the interests protected by the Section 481 and it shall define method of execution of the act.* *In the event that an act is executed pursuant to the legal rules of a foreign country without court decision made pursuant to the Section 539, par. 2, such act is considered as executed contrary to the SK legal regulation.* *Par. 3: Existence of dual criminality in general does not represent condition of realization of legal assistance carrying out the request.* *Provision regulates exception to this rule in the cases where court order is required for producing evidence.* *Examination of dual criminality is conditioned by the fact that it concerns*

	acts representing interference with human rights and fundamental freedoms and the realization of such acts is limited by court decision within criminal proceedings on criminal act. In the SK territory it is not permitted to interfere with these rights within proceedings on an act which would not be criminal act pursuant to the SK law.
Article 26 – Spontaneous information 1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter. 2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	**SEC. 484 of the Code of Criminal Procedure Act no 301/2005 Coll.** **Sending requests for information by means of Interpol** (1) Pursuant to this Part, requests may be sent to foreign country as well as received from it also by means of International Criminal Police Organization (hereinafter referred to as "Interpol"), in particular in the cases of urgent matters. (2) By means of Interpol, also information and data may be exchanged concerning the time and further details in relation to the transfer, taking over or transport of a person or thing pursuant to the Section 485. Spontaneous information exchange is regulated also in the Article 7, Convention on Mutual Assistance in Criminal Matters between EU Countries drawn up by the Council in accordance with the Article 34, Treaty Establishing the European Union (Notifications by the Ministry of Foreign Affairs, no. 572/2006, Coll.).
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	**SEC. 479 of the Code of Criminal Procedure Act no 301/2005 Coll., Mutuality/reciprocity** (1) If a requesting country is not bound by an international treaty then the Slovak authorities may handle its request if a requesting country shall guarantee that it shall handle similar request by the Slovak authority, and if handling/execution of a foreign country's request is not bound/conditioned by existence of international treaty. Fulfilment of the condition stated in the first

responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times. 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party. 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities. 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary. 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly. 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly	sentence shall not be examined in the case of foreign authority's request for service of a document on a person in the territory of the Slovak Republic. (2) If a requested country that is not bound by an international treaty, requests mutuality/reciprocity as a condition for executing the Slovak authority's request, then the Ministry of Justice may give reciprocity guarantee to the requested country as for handling similar request by requested country and upon a condition that no international treaty existence is required for carrying out such request

inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party. b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol). c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so. d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party. e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.	
Article 28 – Confidentiality and limitation on use 1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or b not used for investigations or proceedings other than those stated in the request. 3 If the requesting Party cannot comply with a condition referred to in	**SEC. 482 (2) of the Code of Criminal Procedure Act no 301/2005 Coll., Protection and use of information** Slovak authorities shall not publish nor provide/furnish no information nor evidence obtained from foreign authority on the basis of a request made according to this Part or in connection with it, and they shall not use it for any other purpose but that one for which they had been sent or requested if they are bound so by an international treaty or if the information and evidence was provided to them only upon promise of fulfillment of this condition; this does not apply if a foreign authority gives consent with publication or with any other use of information or evidence.

paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it. 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.	
Article 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 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.	**SEC. 551 of the Code of Criminal Procedure Act no 301/2005 Coll.**

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. 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.	**SEC. 551 of the Code of Criminal Procedure Act no 301/2005 Coll.**
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	**SEC. 537 of the Code of Criminal Procedure Act no 301/2005 Coll.** **Method and form of handling a request** (1) Slovak authorities shall execute a request made by foreign

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.	authorities in a manner stipulated by this Act or by an international treaty. If mutual assistance is made pursuant to an international treaty in a manner that is not regulated in this Act, then a competent prosecutor shall decide on a method of executing legal assistance. (2) Upon request by foreign authority, the requested legal assistance may be executed pursuant to the legal rule of requesting country unless the requested procedure is contrary to the interests protected by the provision of the Section 481. (3) In order to execute a request pursuant to the Section 539, par. 1, it is required that the act in relation to which the request is made, should be criminal act not only pursuant to the legal order of the requesting country, but also pursuant to the legal order of the Slovak Republic. Explanatory comments on the provision of the Section 537, Code of Criminal Procedure of the Slovak Republic (extract): *The mentioned provision explicitly expresses the basic principle of executing legal assistance pursuant to the law of the requested country (lex fori).* *It regulates the extent/scope of the legal assistance awarded so that it restricts/limits it by means of legal regulation of this Act or an international treaty. Upon request by foreign authorities, competent SK authorities may execute in principle any act they are competent to carry out within criminal proceedings conducted in the Slovak Republic or any act regulated by an international treaty. Extent of mutual assistance so defined is also limited by the following elements:* - *in absence of international treaty, actual reciprocity is a prerequisite of carrying out legal assistance i.e. competent authorities of the requesting country are expected to provide the same type of legal assistance as they are requesting for in a similar case,* - *execution of some specific legal assistance acts is conditioned by contractual reciprocity (Section 544, 551), the execution of them is*

	excluded in absence of contractual regulation, - *no significant protected SK interest shall be hindered through execution of requested acts (section 481).* *If requesting authority requests execution of an act pursuant to an international treaty by which SK is bound, whilst the requested method is not regulated in this Act, competent prosecutor shall decide on a manner/method of execution of legal assistance act (Section 538, par.2).* *If requesting authority requests for execution of an act on the basis of an international treaty containing regulation of specific procedure/method that is more detailed or different from domestic legal order regulation, then the act shall be executed pursuant to the international treaty and competent prosecutor shall decide on modalities of carrying out of the act (Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters).* *The provision of the par. 2 admits/allows execution of the legal assistance act pursuant to the legal order of a foreign country, unless such method is contrary to the important protected interests of the Slovak Republic (Section 481) that represents breaching of the basic principle lex fori.* *In such case, competent prosecutor is obliged to submit to the court a request for decision pursuant to the Section 539, par. 2. Court shall decide on existence, absence of conflict with the interests protected by the Section 481 and it shall define method of execution of the act.* *In the event that an act is executed pursuant to the legal rules of a foreign country without court decision made pursuant to the Section 539, par. 2, such act is considered as executed contrary to the SK legal regulation.* *Par. 3: Existence of dual criminality in general does not represent condition of realization of legal assistance carrying out the request.* *Provision regulates exception to this rule in the cases where court order is required for producing evidence.* *Examination of dual criminality is conditioned by the fact that it concerns acts representing interference with human rights and fundamental freedoms and the realization of such acts is limited by court decision within criminal proceedings on criminal act. In the SK territory it is not permitted to interfere with these rights within proceedings on an act which would not be criminal act pursuant to the SK law.*

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.	SEC. 537 of the Code of Criminal Procedure Act no 301/2005 Coll. **SEC. 537 of the Code of Criminal Procedure Act no 301/2005 Coll.** **Method and form of handling a request** (1) Slovak authorities shall execute a request made by foreign authorities in a manner stipulated by this Act or by an international treaty. If mutual assistance is made pursuant to an international treaty in a manner that is not regulated in this Act, then a competent prosecutor shall decide on a method of executing legal assistance. (2) Upon request by foreign authority, the requested legal assistance may be executed pursuant to the legal rule of requesting country unless the requested procedure is contrary to the interests protected by the provision of the Section 481. (3) In order to execute a request pursuant to the Section 539, par. 1, it is required that the act in relation to which the request is made, should be criminal act not only pursuant to the legal order of the requesting country, but also pursuant to the legal order of the Slovak Republic. Explanatory comments on the provision of the Section 537, Code of Criminal Procedure of the Slovak Republic (extract): *The mentioned provision explicitly expresses the basic principle of executing legal assistance pursuant to the law of the requested country (lex fori).* *It regulates the extent/scope of the legal assistance awarded so that it restricts/limits it by means of legal regulation of this Act or an international treaty. Upon request by foreign authorities, competent SK authorities may execute in principle any act they are competent to carry out within criminal proceedings conducted in the Slovak Republic or any act regulated by an international treaty. Extent of mutual assistance so defined is also limited by the*

	following elements: - *in absence of international treaty, actual reciprocity is a prerequisite of carrying out legal assistance i.e. competent authorities of the requesting country are expected to provide the same type of legal assistance as they are requesting for in a similar case,* - *execution of some specific legal assistance acts is conditioned by contractual reciprocity (Section 544, 551), the execution of them is excluded in absence of contractual regulation,* - *no significant protected SK interest shall be hindered through execution of requested acts (section 481).* *If requesting authority requests execution of an act pursuant to an international treaty by which SK is bound, whilst the requested method is not regulated in this Act, competent prosecutor shall decide on a manner/method of execution of legal assistance act (Section 538, par.2).* *If requesting authority requests for execution of an act on the basis of an international treaty containing regulation of specific procedure/method that is more detailed or different from domestic legal order regulation, then the act shall be executed pursuant to the international treaty and competent prosecutor shall decide on modalities of carrying out of the act (Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters).* *The provision of the par. 2 admits/allows execution of the legal assistance act pursuant to the legal order of a foreign country, unless such method is contrary to the important protected interests of the Slovak Republic (Section 481) that represents breaching of the basic principle lex fori.* *In such case, competent prosecutor is obliged to submit to the court a request for decision pursuant to the Section 539, par. 2. Court shall decide on existence, absence of conflict with the interests protected by the Section 481 and it shall define method of execution of the act.* *In the event that an act is executed pursuant to the legal rules of a foreign country without court decision made pursuant to the Section 539, par. 2, such act is considered as executed contrary to the SK legal regulation.* *Par. 3: Existence of dual criminality in general does not represent condition of realization of legal assistance carrying out the request.* *Provision regulates exception to this rule in the cases where court order is required for producing evidence.*

	Examination of dual criminality is conditioned by the fact that it concerns acts representing interference with human rights and fundamental freedoms and the realization of such acts is limited by court decision within criminal proceedings on criminal act. In the SK territory it is not permitted to interfere with these rights within proceedings on an act which would not be criminal act pursuant to the SK law.
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.	**SEC. 537 of the Code of Criminal Procedure Act no 301/2005 Coll.** **Method and form of handling a request** (1) Slovak authorities shall execute a request made by foreign authorities in a manner stipulated by this Act or by an international treaty. If mutual assistance is made pursuant to an international treaty in a manner that is not regulated in this Act, then a competent prosecutor shall decide on a method of executing legal assistance. (2) Upon request by foreign authority, the requested legal assistance may be executed pursuant to the legal rule of requesting country unless the requested procedure is contrary to the interests protected by the provision of the Section 481. (3) In order to execute a request pursuant to the Section 539, par. 1, it is required that the act in relation to which the request is made, should be criminal act not only pursuant to the legal order of the requesting country, but also pursuant to the legal order of the Slovak Republic. Explanatory comments on the provision of the Section 537, Code of Criminal Procedure of the Slovak Republic (extract): *The mentioned provision explicitly expresses the basic principle of executing legal assistance pursuant to the law of the requested country (lex fori).* *It regulates the extent/scope of the legal assistance awarded so that it*

	restricts/limits it by means of legal regulation of this Act or an international treaty. Upon request by foreign authorities, competent SK authorities may execute in principle any act they are competent to carry out within criminal proceedings conducted in the Slovak Republic or any act regulated by an international treaty. Extent of mutual assistance so defined is also limited by the following elements: - *in absence of international treaty, actual reciprocity is a prerequisite of carrying out legal assistance i.e. competent authorities of the requesting country are expected to provide the same type of legal assistance as they are requesting for in a similar case,* - *execution of some specific legal assistance acts is conditioned by contractual reciprocity (Section 544, 551), the execution of them is excluded in absence of contractual regulation,* - *no significant protected SK interest shall be hindered through execution of requested acts (section 481).* *If requesting authority requests execution of an act pursuant to an international treaty by which SK is bound, whilst the requested method is not regulated in this Act, competent prosecutor shall decide on a manner/method of execution of legal assistance act (Section 538, par.2).* *If requesting authority requests for execution of an act on the basis of an international treaty containing regulation of specific procedure/method that is more detailed or different from domestic legal order regulation, then the act shall be executed pursuant to the international treaty and competent prosecutor shall decide on modalities of carrying out of the act (Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters).* *The provision of the par. 2 admits/allows execution of the legal assistance act pursuant to the legal order of a foreign country, unless such method is contrary to the important protected interests of the Slovak Republic (Section 481) that represents breaching of the basic principle lex fori.* *In such case, competent prosecutor is obliged to submit to the court a request for decision pursuant to the Section 539, par. 2. Court shall decide on existence, absence of conflict with the interests protected by the Section 481 and it shall define method of execution of the act.* *In the event that an act is executed pursuant to the legal rules of a foreign country without court decision made pursuant to the Section 539, par. 2, such*

	act is considered as executed contrary to the SK legal regulation. *Par. 3: Existence of dual criminality in general does not represent condition of realization of legal assistance carrying out the request.* *Provision regulates exception to this rule in the cases where court order is required for producing evidence.* *Examination of dual criminality is conditioned by the fact that it concerns acts representing interference with human rights and fundamental freedoms and the realization of such acts is limited by court decision within criminal proceedings on criminal act. In the SK territory it is not permitted to interfere with these rights within proceedings on an act which would not be criminal act pursuant to the SK law.*
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.	**SEC. 537 of the Code of Criminal Procedure Act no 301/2005 Coll.** **Method and form of handling a request** (1) Slovak authorities shall execute a request made by foreign authorities in a manner stipulated by this Act or by an international treaty. If mutual assistance is made pursuant to an international treaty in a manner that is not regulated in this Act, then a competent prosecutor shall decide on a method of executing legal assistance. (2) Upon request by foreign authority, the requested legal assistance may be executed pursuant to the legal rule of requesting country unless the requested procedure is contrary to the interests protected by the provision of the Section 481. (3) In order to execute a request pursuant to the Section 539, par. 1, it is required that the act in relation to which the request is made, should be criminal act not only pursuant to the legal order of the requesting country, but also pursuant to the legal order of the Slovak Republic. Explanatory comments on the provision of the Section 537, Code of Criminal Procedure of the Slovak Republic (extract):

	The mentioned provision explicitly expresses the basic principle of executing legal assistance pursuant to the law of the requested country (lex fori). *It regulates the extent/scope of the legal assistance awarded so that it restricts/limits it by means of legal regulation of this Act or an international treaty. Upon request by foreign authorities, competent SK authorities may execute in principle any act they are competent to carry out within criminal proceedings conducted in the Slovak Republic or any act regulated by an international treaty. Extent of mutual assistance so defined is also limited by the following elements:* - *in absence of international treaty, actual reciprocity is a prerequisite of carrying out legal assistance i.e. competent authorities of the requesting country are expected to provide the same type of legal assistance as they are requesting for in a similar case,* - *execution of some specific legal assistance acts is conditioned by contractual reciprocity (Section 544, 551), the execution of them is excluded in absence of contractual regulation,* - *no significant protected SK interest shall be hindered through execution of requested acts (section 481).* *If requesting authority requests execution of an act pursuant to an international treaty by which SK is bound, whilst the requested method is not regulated in this Act, competent prosecutor shall decide on a manner/method of execution of legal assistance act (Section 538, par.2).* *If requesting authority requests for execution of an act on the basis of an international treaty containing regulation of specific procedure/method that is more detailed or different from domestic legal order regulation, then the act shall be executed pursuant to the international treaty and competent prosecutor shall decide on modalities of carrying out of the act (Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters).* *The provision of the par. 2 admits/allows execution of the legal assistance act pursuant to the legal order of a foreign country, unless such method is contrary to the important protected interests of the Slovak Republic (Section 481) that represents breaching of the basic principle lex fori.* *In such case, competent prosecutor is obliged to submit to the court a request*

	for decision pursuant to the Section 539, par. 2. Court shall decide on existence, absence of conflict with the interests protected by the Section 481 and it shall define method of execution of the act. *In the event that an act is executed pursuant to the legal rules of a foreign country without court decision made pursuant to the Section 539, par. 2, such act is considered as executed contrary to the SK legal regulation.* *Par. 3: Existence of dual criminality in general does not represent condition of realization of legal assistance carrying out the request.* *Provision regulates exception to this rule in the cases where court order is required for producing evidence.* *Examination of dual criminality is conditioned by the fact that it concerns acts representing interference with human rights and fundamental freedoms and the realization of such acts is limited by court decision within criminal proceedings on criminal act. In the SK territory it is not permitted to interfere with these rights within proceedings on an act which would not be criminal act pursuant to the SK law.*
Article 35 – 24/7 Network 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects. 2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate	With regard to the fact that the Slovak Republic has not ratified the Convention on Cybercrime so far, it also has not fully operating contact points (trained staff as well as necessary equipment) for the purposes of the Convention on Cybercrime within the meaning of the Article 35 of the Convention. Pursuant to the Act no. 211/2000, Coll., on free access to information, as amended (Act on Free Access to Information), every one has right of common access to the published information by means of telecommunication device, in particular by means of Internet, without showing any legal or other reason or interest for which the information is requested. Article 32, letter b) of the Convention on Cybercrime corresponds with the Act no. 428/2002, Coll., on Protection of Personal Data as amended, in the cases where the person concerned gives consent to process his/her personal

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.	data.
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.	