Bulgaria

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Version 01 May 2020

Table of contents

[reference to the provisions of the Budapest Convention]

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

www.coe.int/cybercrime

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

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

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data": For the purposes of this Convention: a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; c "service provider" means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service; d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service	**Criminal code** **Article 93** (Amended, SG No. 28/1982, SG No. 10/1993, SG No. 50/1995, SG No. 62/1997, SG No. 153/1998, SG No. 7/1999) The words and expressions indicated below shall be construed for the purpose of this Code to mean the following: 21. (New, SG No. 92/2002, amended, SG No. 38/2007) A "**computer system**" is any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data. 22. (New, SG No. 92/2002, amended, SG No. 38/2007) "**Computer data**" is any representation of facts, information or concepts in a form suitable for automatic processing, including computer programs. 23. (New, SG No. 92/2002) A "**provider of computerized information services**" is any individual or entity that provides opportunities for communication by means of a computer system or that processes or stores computer data with regard to the above communication service or its users. **Electronic Communications Act** **Art. 248** (2) Subscriber data include: **1. Traffic data** - data necessary for the providing of electronic communications services, for charging, for the formation of the bills of subscribers and to prove their authenticity, including: a) The number of the calling and the called end-user, card number for online payment; b) Start and end of call, specified by date and time to the nearest second, if technically possible,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	and/or if transfer of data – the volume of transferred data for charging purposes; c) The type of service provided; d) Points of interconnection of the call, the start and end of their use, determined by date and time to the nearest second, if technically possible; e) Details of the type of connection or zones - time and geographical, necessary to determine the value of the service; f) The location of the user of a service, provided by mobile network, including the providing of "roaming";
Chapter II – Measures to be taken at the national level	
Section 1 – Substantive criminal law	
Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems	
Article 2 – Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	**Criminal Code** Article 319a (1) (Amended, SG No. 38/2007) Anyone who copies, uses or obtains access to computer data in a computer system without permission, where such is required, shall be punished by a fine of up to BGN three thousand. (2) Where the act under par. 1 has been committed by two or more people, who have previously agreed so to do, the punishment shall be deprivation of liberty of up to one year or a fine of up to BGN three thousand. (3) (Supplemented, SG No. 38/2007) Where the act under par. 1 is repeated or is with regard to data for creation of an electronic signature, the punishment shall be deprivation of liberty of up three years or a fine of up to BGN five thousand. (4) (Amended, SG No. 26/2004, supplemented, SG No. 38/2007) Where acts under paragraphs 1-3 have been committed with regard to information that qualifies as a secret of the State or to another information protected by the law, the punishment shall be deprivation of liberty from one to three years, unless severe punishment has been envisaged. (5) Where grave consequences have occurred as a result of the acts under par. 4, punishment shall be of one to eight years.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 3 – Illegal interception Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	**Criminal Code** Article 171 (1) (Amended, SG. No. 28/1982, SG No. 10/1993) A person who contrary to the law: 1. opens, falsifies, hides or destroys a letter, telegram, sealed papers, package and the like of another person; 2. takes another person's, although opened, letter or telegram for the purpose of obtaining knowledge of their contents, or for the same purpose delivers another person's letter or telegram to someone else; 3. (New, SG No. 92/2002) Who becomes aware of the content of an electronic message not addressed to him/her or prevents such a message from reaching its original addressee shall be punished by deprivation of liberty for up to one year or by a fine from BGN one hundred to three hundred. (2) If the act was perpetrated by an official who availed himself of his official position, the punishment shall by deprivation of liberty for up to two years, and the court may also rule deprivation of the right under Article 37 (1), sub-paragraph 6. (3) (Supplemented, SG No. 92/2002) A person who, by use of special technical means, unlawfully obtains information not addressed to him, communicated over the telephone, telegraph, computer network or another telecommunication means, shall be punished by deprivation of liberty for up to two years. (4) (New, SG No. 38/2007) Where the act under paragraph 3 has been committed with a venal goal in mind or considerable damages have been caused, the punishment shall be deprivation of liberty for up to three years and a fine of up to BGN five thousand. Article 319d (1) (Amended, SG No. 38/2007) Anyone who introduces a computer virus in a computer system or in a computer network, shall be punished by a fine of up to BGN three thousand. (2) (New, SG No. 38/2007) The punishment under par. 1 shall be imposed also on that person who introduces another computer program which is intended to disrupt the work of a computer system or a computer network or to discover, erase, delete, modify or copy computer data without permission, where such is required, as long as it is not a graver crime. (3) (Renumbered from Paragraph 2 and amended, SG No. 38/2007) Where

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	considerable damage has occurred as a result of the act under paras. 1 and 2 or it has been repeated, the punishment shall be deprivation of liberty of up to three years and a fine of up to BGN one thousand.
Article 4 – Data interference 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	**Criminal Code** Article 171a(New, SG No. 26/2010) (1) (Amended and supplemented, SG No. 24/2015, effective 31.03.2015) A person who unlawfully acquires, stores, discloses or disseminates data as those collected, processed, kept or used as per the Electronic Communications Act, shall be punished by imprisonment up to three years or probation. (2) If the act under paragraph 1 was committed for a venal goal, the punishment shall be imprisonment from one to six years. Article 212a (New, SG No. 92/2002) (1) (Amended, SG No. 38/2007) Where an individual, in view of providing a benefit to him-/herself or another, brings or maintains misleading representations in someone through introducing, modifying, deleting, or erasing computerized data or through the use of an electronic signature of another causes him/her or another harm, shall be punished for computer fraud by deprivation of liberty from one to six years and a fine of up to BGN six thousand (2) (Amended, SG No. 38/2007) The same form and amount of punishment shall be imposed to the individual who, without being entitled thereto, introduces, modifies, or erases computerized data in order to unduly obtain something, that should not go to him. Article 319b (1) (Amended, SG No. 38/2007) Anyone who, without consent by a person administering or using a computer system, installs, modifies, deletes or destroys a computer program or computer data, where the occurrence is not considered insignificant, shall be punished by deprivation of liberty of up to one year or a fine of up to BGN two thousand. (2) Where significant damage or other grave consequences have occurred as a result of an act under par. 1, the punishment shall be a deprivation of liberty of up to two years and a fine of up to BGN three thousand. (3) Where the act under par. 1 has been committed in view of obtaining a material benefit, the punishment shall be deprivation of liberty from one to three years and a fine of up to BGN five thousand. Article 319c (1) (Supplemented, SG No. 38/2007) Anyone who commits the act under art. 319b with regard to data that are provided electronically or upon magnet,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	electronic, optic or other carriers by virtue of the law shall be punished by deprivation of liberty of up to two years and a fine of up to BGN three thousand. (2) Where the act under par. 1 was intended to prevent the fulfilment of an obligation, the punishment shall be deprivation of liberty of up to three years and a fine of up to BGN five thousand.
Article 5 – System interference Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data	**Criminal Code** Article 319b (1) (Amended, SG No. 38/2007) Anyone who, without consent by a person administering or using a computer system, installs, modifies, deletes or destroys a computer program or computer data, where the occurrence is not considered insignificant, shall be punished by deprivation of liberty of up to one year or a fine of up to BGN two thousand. (2) Where significant damage or other grave consequences have occurred as a result of an act under par. 1, the punishment shall be a deprivation of liberty of up to two years and a fine of up to BGN three thousand. (3) Where the act under par. 1 has been committed in view of obtaining a material benefit, the punishment shall be deprivation of liberty from one to three years and a fine of up to BGN five thousand. Article 319c (1) (Supplemented, SG No. 38/2007) Anyone who commits the act under art. 319b with regard to data that are provided electronically or upon magnet, electronic, optic or other carriers by virtue of the law shall be punished by deprivation of liberty of up to two years and a fine of up to BGN three thousand. (2) Where the act under par. 1 was intended to prevent the fulfilment of an obligation, the punishment shall be deprivation of liberty of up to three years and a fine of up to BGN five thousand.
Article 6 – Misuse of devices 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of: i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,	**Criminal Code** Article 319e (1) (Amended, SG No. 26/2004, SG No. 38/2007) Anyone who discloses passwords or codes for access to a computer system or to computer data, and personal data or information which qualifies as secret of the State or another secret protected by the law are thus revealed, shall be punished by deprivation of liberty of up to one year. (2) (Supplemented, SG No. 38/2007) With regard to an act under par. 1, committed with a venal goal in mind, or where it has caused considerable damage or other grave consequences have occurred, punishment shall be

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.	deprivation of liberty of up to three years. Article 319d (1) (Amended, SG No. 38/2007) Anyone who introduces a computer virus in a computer system or in a computer network, shall be punished by a fine of up to BGN three thousand. (2) (New, SG No. 38/2007) The punishment under par. 1 shall be imposed also on that person who introduces another computer program which is intended to disrupt the work of a computer system or a computer network or to discover, erase, delete, modify or copy computer data without permission, where such is required, as long as it is not a graver crime. (3) (Renumbered from Paragraph 2 and amended, SG No. 38/2007) Where considerable damage has occurred as a result of the act under paras. 1 and 2 or it has been repeated, the punishment shall be deprivation of liberty of up to three years and a fine of up to BGN one thousand. Article 348a (New, SG No. 26/2004) (1) The one who, through deceit or any other unlawful means, makes use of a telecommunication network, equipment or service, in order to generate or redirect, to his own or the interest of another, the directed transmission of signals, written text, image, sound, data or messages of any type, through conductors, radio waves, optical or any other transmission environment, shall be punished by deprivation of liberty of up to six years and a fine of up to BGN ten thousand. (2) Where the act under para 1 has been committed: 1. by two or more individuals, who have reached preliminary agreement for its accomplishment, where the latter does not constitute a minor offence; 2. through the use of a non-registered telecommunication device; 3. for a second time, the punishment shall be deprivation of liberty of up to eight years and a fine from BGN one thousand to five thousand. (3) In minor cases falling under para 1 the punishment shall be deprivation of liberty of up to one year or probation. Article 216 (1) (Amended, SG No. 10/1993) A person who unlawfully destroys or endamages movable or real property of another, shall be punished by deprivation of liberty for up to five years.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(2) (New, SG No. 92/2002) An individual who destroys, demolishes or harms his/her property that has been mortgaged or pledged, shall be punished by deprivation of liberty of up to five years and a fine of up to BGN two thousand (3) (New, SG No. 92/2002) Where an individual, through acquiring illegal access to a computer relevant to an enterprise, establishment, legal entity or individual, destroys or causes harm to the property of another, shall be punished by deprivation of liberty from one to six years and a fine of up to BGN ten thousand (4) (Amended, SG No. 28/1982, SG No. 10/1993, renumbered from Paragraph 2, SG No. 92/2002) In minor cases the punishment shall be deprivation of liberty for up to six months or a fine from BGN one hundred to three hundred. (5) (Supplemented, SG No. 62/1997, renumbered from Paragraph 3, SG No. 92/2002, amended and supplemented, SG No. 26/2004) If considerable damages have been caused or other grave consequences have set in or if the act has been committed by a person under Article 142, paragraph (2), subparagraphs 6 and 8, or where the act is associated with the destruction or damaging of telecommunication network elements, the punishment shall be deprivation of liberty for up to ten years, and the court may also rule deprivation of rights under Article 37, paragraph 1, sub-paragraphs 6 and 7. (6) (Amended, SG No. 10/1993, renumbered from Paragraph 4, amended, SG No. 92/2002) If the act under paragraphs (1), (2), (3) and (5) has been committed through negligence, the punishment shall be deprivation of liberty for up to two years or a fine of BGN one hundred to three thousand.
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.	**Criminal Code** Article 212a (New, SG No. 92/2002) (1) (Amended, SG No. 38/2007) Where an individual, in view of providing a benefit to him-/herself or another, brings or maintains misleading representations in someone through introducing, modifying, deleting, or erasing computerized data or through the use of an electronic signature of another causes him/her or another harm, shall be punished for computer fraud by deprivation of liberty from one to six years and a fine of up to BGN six thousand (2) (Amended, SG No. 38/2007) The same form and amount of punishment shall be imposed to the individual who, without being entitled thereto,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	introduces, modifies, or erases computerized data in order to unduly obtain something, that should not go to him. Article 319b (1) (Amended, SG No. 38/2007) Anyone who, without consent by a person administering or using a computer system, installs, modifies, deletes or destroys a computer program or computer data, where the occurrence is not considered insignificant, shall be punished by deprivation of liberty of up to one year or a fine of up to BGN two thousand. (2) Where significant damage or other grave consequences have occurred as a result of an act under par. 1, the punishment shall be a deprivation of liberty of up to two years and a fine of up to BGN three thousand. (3) Where the act under par. 1 has been committed in view of obtaining a material benefit, the punishment shall be deprivation of liberty from one to three years and a fine of up to BGN five thousand.
Article 8 – Computer-related fraud Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.	**Criminal Code** Article 212a (New, SG No. 92/2002) (1) (Amended, SG No. 38/2007) Where an individual, in view of providing a benefit to him-/herself or another, brings or maintains misleading representations in someone through introducing, modifying, deleting, or erasing computerized data or through the use of an electronic signature of another causes him/her or another harm, shall be punished for computer fraud by deprivation of liberty from one to six years and a fine of up to BGN six thousand (2) (Amended, SG No. 38/2007) The same form and amount of punishment shall be imposed to the individual who, without being entitled thereto, introduces, modifies, or erases computerized data in order to unduly obtain something, that should not go to him.
Title 3 – Content-related offences	
Article 9 – Offences related to child pornography 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system;	**Criminal Code** Article 159 (Amended, SG No. 28/1982, SG No. 10/1993, SG No. 62/1997, SG No. 92/2002) (1) (Amended, SG No. 38/2007) A person who produces, displays, presents, broadcasts, distributes, sells, rents or otherwise circulates a pornographic material, shall be punished by deprivation of liberty of up to one year and a fine of BGN one thousand (1,000) to three thousand (3,000).

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct 3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.	(2) (New, SG No. 38/2007) A person who distributes through Internet a pornographic material, shall be punished by deprivation of liberty of up to two years and a fine of BGN one thousand to three thousand. (3) (Renumbered from paragraph 2 and amended, SG No. 38/2007) An individual who displays, presents, offers, sells, rents or distributes in another manner a pornographic material to a person who has not turned 16 years of age, shall be punished by deprivation of liberty of up to three years and a fine of up to BGN five thousand (5,000). (4) (Amended, SG No. 75/2006, renumbered from Paragraph 3 and amended, SG No. 38/2007) Regarding acts under paras. 1-3, where a person who has not turned 18 years of age, or a person who looks like such a person, has been used in the creation of a pornographic material, the punishment shall be deprivation of liberty of up to six years and a fine of up to BGN eight thousand (8,000). (5) (Renumbered from paragraph 4 and amended, SG No. 38/2007) Where acts under paras. 1 - 4 have been committed at the orders or in implementing a decision of an organized criminal group, punishment shall be deprivation of liberty from two to eight years and a fine of up to BGN ten thousand (10,000), the court being also competent to impose confiscation of some or all the possessions of the perpetrator. (6) (Renumbered from paragraph 5 and amended, SG No. 38/2007) A person who possesses or provides for himself or for another person through a computer system or in another manner a pornographic material in whose creation a person who has not turned 18 years of age has been used or a person who looks like such a person, shall be punished by deprivation of liberty of up to one year or a fine of up to BGN two thousand. (7) (Renumbered from paragraph 6, SG No. 38/2007) The object of criminal activity shall be expropriated to the benefit of the State, and where it is not found or has been disposed of, its money equivalent shall be awarded.
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	**Criminal Code** Article 172a (New, SG No. 50/1995) (1) (Amended, SG No. 62/1997, amended, SG No. 75/2006) A person who makes records, reproduces, distributes, broadcasts or transmits, or makes any other use the object of a copyright or neighbouring right without the consent of

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	the owner of holder of such right as required by law, shall be punished by deprivation of liberty for up to five years and a fine of up to BGN 5,000. (2) (Amended, SG No. 62/1997, amended, SG No. 75/2006) Anyone who, without consent from the person required by law, detains material carriers containing the object of copyright or a neighbouring right, amounting to a large-scale value, or who detains a matrix for the reproduction of such carriers, shall be punished by deprivation of liberty from two to five years and a fine of BGN 2,000 to BGN 5,000. (3) (Amended, SG No. 62/1997, amended, SG No. 75/2006) If the act under Paragraphs (1) and (2) has been repeated or considerable damaging consequences have occurred, the punishment shall be deprivation of liberty from one to six years and a fine of BGN 3,000 to BGN 10,000. (4) (New, SG No. 75/2006) Where the act under para 2 amounts to a particularly large-scale value, the punishment shall be deprivation of liberty from two to eight years and a fine of BGN 10,000 to BGN 50,000. (5) (Renumbered from Paragraph 4, SG No. 75/2006) For minor cases the perpetrator shall be punished under the administrative procedure in compliance with the Copyright and Neighbouring Rights Act. (6) (Renumbered from Paragraph 5, amended, SG No. 75/2006) The object of the crime shall be appropriated in favour of the state, irrespective of the fact whose property it is. Article 172b (New, SG No. 75/2006) (1) Anyone who, without consent from the owner of the exclusive right thereupon, makes use in commercial operations of a trademark, industrial model, a variety of plant or race of animal, making the object of said exclusive right, or makes use of a geographical indication or a counterfeit thereof without a legal justification, shall be punished by deprivation of liberty of up to five years and a fine of up to BGN 5,000. (2) Where the act under para 1 is repeated or significant damages have been caused, the punishment shall be deprivation of liberty from five to eight years and a fine from BGN 5,000 to BGN 8,000. (3) The object of the crime shall be taken to the benefit of the state, irrespective of the fact whose property it is, and it shall then be destroyed.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Article 173 (1) (Amended, SG No. 10/1993) A person who publishes or uses under his own name or under a pen name the work of another person in the field of science, literature or arts or a considerable part thereof, shall be punished by deprivation of liberty for up to two years or by a fine from BGN one hundred to three hundred (2) (Amended, SG No. 81/1999) By the same punishment shall also be punished the person who presents for registration or registers in his own name invention, workable model or industrial design of another person. Article 174 A person who, by abusing his official position, gets himself included as a co-author of an invention, workable model or industrial design or of a work of science, literature or arts, without having taken part in the creative work for its elaboration, shall be punished by deprivation of liberty for up to two years or by a fine from BGN one hundred to three hundred, as well as by public censure.
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.	**Criminal Code** Article 20 (1) Accomplices in the perpetration of intentional crime shall be: perpetrators, abettors and accessories. (2) A perpetrator shall be a person who took part in the perpetration itself of the crime. (3) An abettor shall be a person who intentionally incited another to commit a crime. (4) An accessory shall be a person who intentionally facilitated the perpetration of a crime through advice, explanations, promises to render assistance after the act, removal of obstacles, supply of means or in any other way. Article 21 (1) All accomplices shall be punished by the punishment provided for the perpetrated crime, with due consideration of the nature and degree of their participation. (2) Abettors and accessories shall be held responsible only for what they have intentionally abetted or by what they have assisted the perpetrator. (3) Where because of certain personal characteristics or attitude of the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	perpetrator the law treats the perpetrated act as a crime, liable for this crime shall be both the abettor and the accessory with respect of whom such circumstances do not exist. (4) The special circumstances, due to which the law excludes, reduces or increases the punishment for some of the accomplices, shall not be taken into account for the remaining accomplices with respect to whom such circumstances do not exist. Article 22 (1) The abettor and the accessory shall not be punished, if of their own accord they have given up further participation and hindered the perpetration of the act or averted the occurrence of criminal consequences. (2) In such cases the provisions of Article 19 shall apply, respectively.
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. 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	**Administrative Violations and Sanctions Act** Article 83a(New, SG, No. 79/2005) (1) A legal person, which has enriched itself or would enrich itself from a crime under Articles 108a, 109, 110 (preparations for terrorism), Articles 142143a , 159159c, 209212a,213a, 214 , 215, 225c, 242, 250, 252, 253, 254, 254b, 256, 257, 280, 283, 301307 , 319a319f, 320321a and 354a354c of the Criminal Code , as well as from all crimes, committed under orders of or for implementation of a decision of an organized criminal group, when they have been committed by: 1. an individual, authorized to formulate the will of the legal person; 2. an individual, representing the legal person; 3. an individual, elected to a control or supervisory body of the legal person, or 4. an employee, to whom the legal person has assigned a certain task, when the crime was committed during or in connection with the performance of this task, shall be punishable by a property sanction of up to BGN 1,000,000, but not less than the equivalent of the benefit, where the same is of a property nature; where the benefit is no of a property nature or its amount can not be established, the sanction shall be from BGN 5,000 to 100,000. (2) The property sanction shall also be imposed on the legal person in the cases, when the persons under paragraph 1, items 1, 2 and 3 have abetted or assisted the commission of the above acts, as well as when the said acts were stopped at the stage of attempt. (3) The property sanction shall be imposed regardless of the materialization of the criminal responsibility of the perpetrator of the criminal act under paragraph 1. (4) The benefit or its equivalent shall be confiscated in favour of the state, if not subject to return or restitution, or forfeiture under the procedure of the Criminal Code .

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(5) Property sanctions under paragraph 1 shall not be imposed on states, state bodies and local self-government bodies, as well as on international organizations. Article 83b(New, SG, No. 79/2005) (1) Proceedings under Article 83a shall be initiated upon motivated proposal of the respective prosecutor to the district court: 1. following the entry of the indictment; or 2. when the criminal proceedings may not be initiated or the proceedings initiated were abandoned on the legal grounds that: a) the perpetrator shall not bear criminal responsibility because of amnesty; b) criminal responsibility has expired due to legal prescription, provided for by law; c) the perpetrator has passed away; d) upon commission of the crime, the perpetrator has suffered a permanent mental disorder, which rendered him unanswerable. (2) The proposal must include: 1. description of the crime, the circumstances, in which it was committed and the presence of a causal link between it and the benefit for the legal person; 2. type and amount of the benefit; 3. name, purposes of activity, corporate seat and management address of the legal person; 4. personal details of the individuals, representing the legal person; 5. personal details of the individuals, accused or convicted for the crimes; 6. description of the written materials or of certified copies thereof, which establish the circumstances under items 1 and 2; 7. list of the individuals to be subpoenaed; 8. date and location of its drawing up, the name, position and the signature of the prosecutor. (3) A transcript for the legal person shall be attached to the proposal. Article 83c(New, SG, No. 79/2005) The prosecutor shall be entitled to request the court to take measures for securing the property sanctions against the legal person under the procedure of the Code of Civil Procedure . Article 83d (New, SG, No. 79/2005) The court shall review the proposal in an open meeting with the participation of the prosecutor. Article 83e (New, SG, No. 79/2005) The court shall review the case within the set of circumstances, described in the proposal and based on the evidence collected shall judge on: 1. whether the legal person has derived an illegal benefit; 2. does a connection exist between the perpetrator of the criminal act and the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	legal person; 3. does a connection exist between the criminal act and the benefit for the legal person; 4. what is the amount of the benefit, if of a property nature; Article 83f (New, SG, No. 79/2005) (1) The court shall deliver a judgment for imposing the property sanction after the entry into force of the conviction or of a decision under Article 97(4) of the Criminal Procedure Code (repealed) and after proving the circumstances under Article 83e. (2) The decision must contain data regarding the legal person, the origin, type and amount of the benefit, the amount of the property sanction imposed. (3) As regards cases, posing factual or legal complexities, the motives may be drafted even after delivery of the decision, but not later than 15 days. (4) An appeal on the merits may be lodged against the decision before the respective appellate court within 14 days of communication of the decision. (5) The respective appellate court shall review the appeal under the procedure of the Code of Civil Procedure. Its ruling shall be final.
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.	See previous answers
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer	**Special intelligence means** **Criminal Procedure Code** Article 172 Material objective forms of evidence prepared with the use of special intelligence means (1) Pre-trial bodies may use the following special intelligence means: technical means - electronic and mechanical devices and substances that serve to document operations of the controlled persons and sites, as well as operational techniques - observation, interception, shadowing, penetration, marking and verification of correspondence and computerised information, controlled delivery, trusted transaction and investigation through an officer under cover.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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	(2) Special intelligence means shall be used where this is required for the investigation of serious criminal offences of intent under Chapter one , Chapter two , Sections I, II, IV, V, VIII, and IX, Chapter five , Sections I - VII, Chapter six , Section II - IV, Chapter eight , Chapter nine "a" , Chapter eleven , Sections I - IV, Chapter twelve , Chapter thirteen , and Chapter fourteen , as well as with regard to criminal offences under Article 219 , para 4, proposal 2, Article 220 , para 2, Article 253 , Article 308, paras 2, 3 , and 5, sentence two, Article 321 , Article 321a, Article 356k and 393 of the Special Part of the Criminal Code, where the irrelevant circumstances cannot be established in any other way or this would be accompanied by exceptional difficulties. (3) Computer information service providers shall be under the obligation to provide assistance to the court and pre-trial authorities in the collection and recording of computerized data through the use of special technical devices only where this is required for the purposes of detecting crimes under paragraph 2 (4) The special intelligence means of controlled delivery and trusted transaction may be used to collect material evidence, whereas undercover officers shall be interrogated as witnesses. (5) The materials under paragraphs 1-4 shall be enclosed with the case file.
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other	**Criminal Procedure Code** Article 173 Request for use of special intelligence means (1) A written reasoned request for the use of special intelligence means in a specific case at pre-trial proceedings shall be filed by the prosecutor supervising the investigation to the court. (2) The request must set out: 1. Information about the criminal offence for the investigation of which the use of special intelligence means is required; 2. A description of the action taken so far and its outcomes; 3. Information about the persons or sites in respect to which special intelligence means are to be applied; 4. Operational techniques to be applied; 5. The duration of use.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(3) Where the request is for investigation through an officer under cover, a written declaration by the officer shall be enclosed with it, stating that he/she has been informed of his duties and the objectives of the specific investigation. (4) In urgent cases where this is the only possible way to conduct investigation, an officer under cover may also be used following an order of the prosecutor supervising the investigation. The activity of the officer under cover shall terminate where within 24 hours no authorisation is given by the respective court, which shall also rule with respect to the storage or destruction of the information collected. (5) In cases under Article 123, para 7 written consent from the person in respect to whom special intelligence means are to be used shall also be enclosed with the request. Article 174 Authorisation to use special intelligence means (1) The authorisation for use of special intelligence means shall be given in advance by the Chairperson of the respective District Court or by a Deputy Chairperson explicitly authorized thereby. (2) The authorisation for use of special intelligence means in respect of the military shall be given in advance by the Chairperson of the respective military court or by a Deputy Chairperson explicitly authorised thereby. (3) The body under para 1 and 2 shall rule immediately following receipt of a request in a written reasoned order. (4)Under the conditions and procedure of paras 1 and 2, authorisation for use of special intelligence means may be given as well by the Chairperson of the respective Appellate Court or by a Deputy Chairperson explicitly authorised thereby, should the body pursuant to paragraphs (1) and (2) refuse to grant the requested authorisation. (5) An order for investigation through an officer under cover must specify the criminal offence in respect to which investigation is authorised, officer identity data, cover identity data and an identification number. (6) A special register shall be kept in the respective court for the requests made and the authorisations issued under paras 1 and 2, which shall not be public. Article 175 Procedure and term for the application of special intelligence means for the needs of criminal proceedings (1) The special intelligence means shall be applied in pursuance of the Special Intelligence Means Act only by the respective services of the Ministry of Interior. (2) The Minister of Interior shall issue an order in writing for the application of special intelligence means by the services under paragraph (1), on the grounds

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	of the authorisation under Article 174. (3) The term for application of special intelligence means may not exceed two months. (4) Where needed, the term under para 3 may be extended in pursuance of Article 174, by no more than four months. (5) The application of special intelligence means shall be discontinued when: 1. the objective that has been set, is achieved; 2. the use of such means bears no results; 3. the term for their use has expired. (6) In the event of discontinuing the use of special intelligence means the body that has issued the authorisation should be notified immediately in writing, with indication of the reasons thereof. In cases under para 5, item 2, it shall order the destruction of the primary material carrier containing the information collected. Article 176 Preparation of material objective forms of evidence obtained through the use of special intelligence means When using special intelligence means, material objective forms of evidence shall be prepared in two copies and within 24 hours of their preparation they shall be sealed and handed over to the prosecutor who has requested the authorisation or, respectively, the court, which has given it. Article 177 Evidentiary force of data obtained through the use of special intelligence means (1) The indictment and the sentence may not be based only on data from special intelligence means or on these only and on testimony of witnesses with a secret identity. (2) No results obtained outside the request made under Article 173 can be used in criminal proceedings, unless they contain information about another serious crime of intent under Article 172, para 2. **Special Intelligence Means Act** Article 3 (1) Special intelligence means shall be used to prevent or detect grave crimes as stipulated by the Criminal Procedure Code, should the case necessitate it, where there are no other means to collect the necessary information. (2) In the cases, referred to in paragraph (1) above, the special intelligence means shall be used to preserve pieces of material evidence pursuant to legal provisions and procedure.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Article 4 Pursuant to the provisions of this Act, special intelligence means may also be used with regard to activities, concerning the protection of the national security. Article 12 (1) Special intelligence means shall be used with regard to: 1. Persons who are reported to, and for whom there are reasonable grounds to presume that they are preparing to commit, are committing, or have committed grave crimes; 2. Persons whose activities are reported, and there are reasonable grounds to presume that they are being manipulated by the persons, referred to in Item 1 above, without being aware of the criminal nature of the activities perpetrated; 3. Persons and facilities related to national security; 4. (new, SG No. 109/2008) facilities for identifying the persons referred to in item 1 or 2 above. (2) Special intelligence means may be used for the protection of the life and the property of persons, who have consented to this in writing. Article 34a(New, SG No. 109/2008) (1) The application and use of special intelligence means shall be controlled by: 1. the Minister of Interior, where special intelligence means are applied and used by structures of the Ministry of Interior; 2. the Chairperson of the State Agency for National Security, where special intelligence means are applied and used by structures of the State Agency for National Security. (2) The heads of the structures referred to in Article 20, paragraph (1) shall exert control with regard to the legality of the application of special intelligence means. Article 34b (New, SG No. 109/2008, amended, SG No. 88/2009) (1) The National Assembly shall, through a committee appointed in accordance with the rules on its organisation and activities, perform parliamentary control and monitoring of the procedures of permission, application and use of special intelligence means, storage and destruction of information obtained through such means, as well as protection of citizens' rights and freedoms against illegal use of special intelligence means. (2) By the 31st day of May every year the Committee referred to in paragraph (1) shall submit to the National Assembly a report on the activities performed, which shall contain summarised information on the permission,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	application and use of special intelligence means, the storage and destruction of the information obtained through such means, as well as the protection of citizens' rights and freedoms against illegal use of special intelligence means. Article 34g (New, SG No. 109/2008) (1) (Redesignated from Article 34g, amended, SG No. 88/2009) For the purposes of its activities, the Committee referred to in Article 34b shall have the right: 1. to require, within its competence, information from the bodies and structures referred to in Articles 13, 15 and 20; 2. to check whether the registers of the bodies and structures referred to in Articles 13, 15 and 20 are duly kept with regard to their activities provided for by law, including the stored requests, permissions and instructions regarding the use and application of special intelligence means, as well as the storage and destruction of information obtained through such means; 3. to access the premises where the documents related to the use and application of special intelligence means are stored and the premises where the information obtained through such means is stored and destroyed; 4. (amended, SG No. 88/2009) to make proposals for improving the procedures of use and application of special intelligence means, as well as the storage and destruction of the information obtained through such means; 5. (repealed, SG No. 88/2009). (2) (New, SG No. 88/2009) In case there is evidence of illegal use and application of special intelligence means, respectively storage or destruction of information obtained through such means, the Committee referred to in Article 34b shall refer to the prosecution bodies and heads of the bodies referred to in Articles 13, 15 and 20. Article 34h (New, SG No. 109/2008, amended, SG No. 88/2009) (1) The Committee referred to in Article 34b shall ex officio inform citizens where special intelligence means have been applied against them illegally. (2) Citizens shall not be informed in case such informing would: 1. compromise the goals referred to in Article 3 or Article 4; 2. pose the risk of disclosure of the operative methods or technical means; 3. pose a threat to the life or health of the undercover officer or of his/her relatives in an ascending or descending line, siblings, spouse or other people with whom he/she is in especially close relations, where the threat stems from the tasks assigned.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	Preservation orders are possible under the broad powers defined in Article 159 of the Criminal Procedure Code which obliges legal and physical persons to "preserve and hand over" computerized data, including traffic data and other objects that may be of significance to the case. This is ordered by a court or, during pre-trial proceedings, by a prosecutor or the police. It pertains to all types of data, any crime and any legal or physical person In addition, search and seizure powers may be used. Moreover, data retention is regulated in the Bulgarian Electronic Communication Act. The powers used for expedited preservation at the domestic level can also be applied for international requests. A 24/7 contact point has been established at the Cybercrime Section, General Directorate for Combating Organized Crime, Ministry of the Interior. **Criminal Procedure Code** Article 159 Obligation to hand over objects, papers, computerised data, data about subscribers to computer information service and traffic data Upon request of the court or the bodies of pre-trial proceedings, all institutions, legal persons, officials and citizens shall be obligated to preserve and hand over all objects, papers, computerized data, including traffic data, that may be of significance to the case.
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.	Preservation and partial disclosure orders are possible under the broad powers defined in Article 159 of the Criminal Procedure Code which obliges legal and physical persons to "preserve and hand over" computerized data, including traffic data and other objects that may be of significance to the case. Traffic data is also retained under data retention regulations. Regarding international requests (Article 30 Budapest Convention): There are no special provisions for partial disclosure for domestic or international purposes. For international requests Bulgaria uses general provisions to obtain the full disclosure at the domestic level but discloses to foreign authorities only the partial information needed. A formal MLA request is not necessary.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Criminal Procedure Code** Article 159 Obligation to hand over objects, papers, computerised data, data about subscribers to computer information service and traffic data Upon request of the court or the bodies of pre-trial proceedings, all institutions, legal persons, officials and citizens shall be obligated to preserve and hand over all objects, papers, computerized data, including traffic data that may be of significance to the case.
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: 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.	Domestic production order can be delivered according to the provisions in the Electronic Communications Act – art. 251b and art. 251c only with regard to investigation of a serious crime (punishable by five years or more) or with regards to national security. The domestic production order has to be a court order. The law only regulates the orders to providers which are registered with the Commission on Electronic Communication. There are no regulations on orders to foreign service providers. Electronic Communications Act Art. 251b. (New - SG. 24 of 2015, effective 03.31.2015) (1) The enterprises providing public electronic communications networks and / or services store for 6 months data generated or processed in the process of their activities, which are necessary for: 1. trace and identify the source of the connection; 2. identification of the destination of the connection; 3. identify the date, time and duration of the connection; 4. identification of the type of connection; 5. identification of electronic communication device of the user or what presents to his terminal; 6. establishment of an identifier of the used cells. (2) The data under para. 1 shall be kept for the needs of national security and the prevention, detection and investigation of serious crime. (3) Other data, including revealing the content of the messages can not be stored in this way. (4) The data under para. 1 is processed and stored in accordance with the requirements of the protection of personal data.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Art. 251c. (New - SG. 24 of 2015, effective 03.31.2015) (1) Right to want to consult the data under Art. 251b para. 1 where data are necessary for the performance of their duties are: 1. Specialized directorates, regional directorates and autonomous territorial departments of the State Agency "National Security"; 2. General Directorate "National Police" General Directorate "Combating Organized Crime" and its territorial units, General Directorate "Border Police" and its territorial units, "Internal Security", the Sofia Directorate of the Interior and the regional directorates of the Ministry of interior; 3. "Military Information" and "Military Police" of the Ministry of Defence; 4. (amend. - SG. 79 of 2015, effective 01.11.2015) The State Agency "Intelligence". (2) Access to the data of art. 251b para. 1 is given after a reasoned written request from the head of the bodies under para. 1 or authorized person, including: 1. The legal basis and purpose for which access is required; 2. The registration number of the file for which the need for a access is required, and user data, when known; 3. The data which should be reflected in the report; 4. The period of time for the report; 5. Complete and comprehensible indication of the facts and circumstances justifying the purpose of art. 251b para. 2; 6. The designated official to whom to provide the data. (3) For the requests the bodies under par. 1 shall keep a special register which should not be public.
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.	**Criminal Procedure Code** **Searches and seizures** Article 159 Obligation to hand over objects, papers, computerised data, data about subscribers to computer information service and traffic data Upon request of the court or the bodies of pre-trial proceedings, all institutions, legal persons, officials and citizens shall be obligated to preserve and hand over all objects, papers, computerized data, including traffic data, that may be of significance to the case.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 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.	Article 160 Grounds for and purpose of the search (1) Should there be sufficient reasons to assume that in certain premises or on certain persons objects, papers or computerized information systems containing computerized data may be found, which may be of significance to the ease, searches shall be conducted for their discovery and seizure. (2) A search may also be conducted for the purpose of finding a person or a body. Article 161 Bodies making decisions on searches and seizures (1) In pre-trial proceedings search and seizure shall be performed with a authorisation by a judge from the respective first instance court or a judge from the first-instance court in the area of which the action is taken, upon request of the prosecutor. (2) In cases of urgency, where this is the only possible way to collect and keep evidence, the bodies of pre-trial proceedings may perform physical examination without authorisation under paragraph 1, the record of the investigative action being submitted for approval by the supervising prosecutor to the judge forthwith, but not later than 24 hours thereafter. (3) In court proceedings a search and seizure shall be performed following a decision of the court which is trying the case. Article 163 Conducting searches and seizures (1) Searches and seizures shall be performed in daytime, except where they can suffer no delay. (2) Before proceeding with a search and seizure, the respective body shall submit the authorisation therefore, and shall ask the objects, papers, and computerized information systems containing computerized data sought to be shown to him/her. (3) The body performing the search shall have the right to forbid those present to contact other persons or each other, as well as to leave the premises until completion of the search. (4) No actions may be undertaken during searches and seizures, which are not necessitated by their purposes. Premises and storerooms shall only be forcefully opened in the case of refusal to be opened, unnecessary damage being avoided. (5) Where in the course of searches and seizures circumstances of the intimate life of citizens are revealed, measures shall be taken as necessary so that they are not be made public.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(6) The objects, papers and computerized information systems containing computerized data seized shall be shown to the certifying witnesses and the other attending persons. Where necessary, these shall be wrapped and sealed at the location where they had been seized. (7) Seizure of computerized data shall be operated through record on paper or another carrier. In case of a paper carrier, each page shall be signed by the persons under Article 132, para 1. In other cases the carrier shall be sealed with a note stating: the case, the body performing the seizure, the location, date, and names of all individuals present under Article 132, para 1 who shall sign it. (8) Carriers prepared in pursuance of para 7 will only be unsealed with the authorisation of the prosecutor for the needs of the investigation, which shall be carried out in presence of certifying witnesses and an expert- technical assistant. In court proceedings carriers shall be unsealed upon decision of the court by an expert technical assistant. Article 164 Search of a person (1) The search of a person in pre-trial proceedings without authorisation by a judge from the respective first instance court or a judge from the first-instance court in the area of which the action is taken shall be allowed: 1. at detention; 2. should there be sufficient grounds to believe that persons who are present at the search have concealed objects or papers of significance to the case. (2) The search of a person shall be performed by an individual of the same gender in the presence of certifying witnesses of the same gender. (3) The record of the performed investigative action shall be submitted for approval to the judge forthwith, but not later than 24 hours thereafter. Article 165 Interception and seizure of correspondence (1) Interception and seizure of correspondence shall be allowed only where this is necessary for disclosure or prevention of serious crime. (2) Interception and seizure of correspondence in pre-trial proceedings shall be performed upon request of the prosecutor with the authorisation of a judge from the respective first instance court or a judge from the court in the area of which the action is taken. (3) In court proceedings search and seizure of correspondence shall be performed by a decision of the court which is trying the case. (4) The interception and seizure of correspondence shall be carried out in

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	pursuance of Article 162, paras 1 - 4. (5)The provisions of paragraphs 1 - 4 shall also apply to searches and seizures of electronic mail.
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 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.	**Special intelligence means** **Criminal Procedure Code** Article 172 Material objective forms of evidence prepared with the use of special intelligence means (1) Pre-trial bodies may use the following special intelligence means: technical means - electronic and mechanical devices and substances that serve to document operations of the controlled persons and sites, as well as operational techniques - observation, interception, shadowing, penetration, marking and verification of correspondence and computerised information, controlled delivery, trusted transaction and investigation through an officer under cover. (2) Special intelligence means shall be used where this is required for the investigation of serious criminal offences of intent under Chapter one , Chapter two , Sections I, II, IV, V, VIII, and IX, Chapter five , Sections I - VII, Chapter six , Section II - IV, Chapter eight , Chapter nine "a" , Chapter eleven , Sections I - IV, Chapter twelve , Chapter thirteen , and Chapter fourteen , as well as with regard to criminal offences under Article 219 , para 4, proposal 2, Article 220 , para 2, Article 253 , Article 308, paras 2, 3 , and 5, sentence two, Article 321 , Article 321a, Article 356k and 393 of the Special Part of the Criminal Code, where the irrelevant circumstances cannot be established in any other way or this would be accompanied by exceptional difficulties. (3) Computer information service providers shall be under the obligation to provide assistance to the court and pre-trial authorities in the collection and recording of computerized data through the use of special technical devices only where this is required for the purposes of detecting crimes under paragraph 2 (4) The special intelligence means of controlled delivery and trusted transaction may be used to collect material evidence, whereas undercover officers shall be interrogated as witnesses. (5) The materials under paragraphs 1-4 shall be enclosed with the case file.
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	**Special intelligence means** **Criminal Procedure Code** Article 172 Material objective forms of evidence prepared with the use of special intelligence means (1) Pre-trial bodies may use the following special intelligence means: technical means - electronic and mechanical devices and substances that serve to

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	document operations of the controlled persons and sites, as well as operational techniques - observation, interception, shadowing, penetration, marking and verification of correspondence and computerised information, controlled delivery, trusted transaction and investigation through an officer under cover. (2) Special intelligence means shall be used where this is required for the investigation of serious criminal offences of intent under Chapter one , Chapter two , Sections I, II, IV, V, VIII, and IX, Chapter five , Sections I - VII, Chapter six , Section II - IV, Chapter eight , Chapter nine "a" , Chapter eleven , Sections I - IV, Chapter twelve , Chapter thirteen , and Chapter fourteen , as well as with regard to criminal offences under Article 219 , para 4, proposal 2, Article 220 , para 2, Article 253 , Article 308, paras 2, 3 , and 5, sentence two, Article 321 , Article 321a, Article 356k and 393 of the Special Part of the Criminal Code, where the irrelevant circumstances cannot be established in any other way or this would be accompanied by exceptional difficulties. (3) Computer information service providers shall be under the obligation to provide assistance to the court and pre-trial authorities in the collection and recording of computerized data through the use of special technical devices only where this is required for the purposes of detecting crimes under paragraph 2 (4) The special intelligence means of controlled delivery and trusted transaction may be used to collect material evidence, whereas undercover officers shall be interrogated as witnesses. (5) The materials under paragraphs 1-4 shall be enclosed with the case file.
Section 3 – Jurisdiction	
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or 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	**Penal Code** Article 3 (1) The Criminal code shall apply to all crimes committed on the territory of the Republic of Bulgaria. (2) The issue of liability of foreign citizens who enjoy immunity with respect to the penal jurisdiction of the Republic of Bulgaria shall be decided in compliance with the norms of international law adopted thereby. Article 4 (1) The Criminal code shall apply to the Bulgarian citizens also for crimes committed by them abroad. (2) (Amended, SG No. 75/2006) No citizen of the Republic of Bulgaria can be

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	transferred to another state or an international court of justice for the purposes of prosecution, unless this has been provided for in an international agreement, which has been ratified, published and entered into force in respect to the Republuc of Bulgaria. Article 5 The Criminal code shall also apply to foreign citizens who have committed crimes of general nature abroad, whereby the interests of the Republic of Bulgaria or of Bulgarian citizens have been affected. Article 6 (1) The Criminal code shall also apply to foreign citizens who have committed abroad crimes against peace and humanity, whereby the interests of another state or foreign citizens have been affected. (2) The Criminal code shall also apply to other crimes committed by foreign citizens abroad, where this is stipulated in an international agreement, to which the Republic of Bulgaria is a party. ……. Article 31 (1) Penally responsible shall be any person of full age - who has completed 18 years of age, and who has perpetrated a crime in the state of being responsible for his acts. (2) A minor - a person who has completed 14 years of age, but has not completed 18 years of age yet - shall be penally responsible if he was able to understand the nature and meaning of the act and to manage his actions. (3) (Amended, SG No. 107/1996) Minors who cannot be considered culpable of their acts shall be admitted by a decision of the court to a correctional boarding school or to another appropriate establishment, should this be found necessary considering the circumstances of the case. (4) With regard to the penal responsibility of minors, the special rules provided by this Code shall be applicable. Article 32 (1) Underage persons who have not completed 14 years of age shall not be held penally responsible. (2) With respect to minors who have committed socially dangerous acts, the relevant educational measures may be applied. Article 33

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(1) Penally responsible shall not be a person, who has acted in a state of insanity - where due to retarded mentality or derangement of his consciousness of prolonged or short duration, the person has not been able to understand the nature and meaning of the act or to manage his actions. (2) (Amended, SG No. 95/1975) No punishment shall be imposed on a person who has committed a crime, where by the pronouncement of the sentence that person falls into a state of deranged consciousness, as a result of which he cannot understand the nature and meaning of his actions or manage them. Such a person shall be subject to punishment if he recovers his health. Article 35 (1) Penal responsibility is personal. (2) A punishment may be imposed only on a person who has committed a crime provided for by the law. (3) The punishment shall correspond to the crime. (4) A punishment for a crime shall be imposed only by the established courts of law.
Chapter III – International co-operation	
Article 24 – Extradition 1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply. 2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them. 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	**EXTRADITON AND EUROPEAN ARREST WARRANT ACT** **Conditions for application of the European Arrest Warrant** **Art. 36. (*) (1)** (amend. – SG 49/10) European Arrest Warrant shall be issued for persons who has committed offences, which carry as per the legislation of the requesting country maximum term of not less than one year imprisonment sentence or a measure requiring detention or another more severe penalty, or if the imposed penalty imprisonment or the requiring detention measure is not shorter than 4 months. **(2)** The surrender on the base of European Arrest Warrant shall be performed, if the offence which the warrant has been issued for, constitutes a offence as per the Bulgarian legislation too. Execution of an European Arrest Warrant related to taxes, custom fees or currency exchange cannot be refused on the ground that the Bulgarian legislation does not stipulate the same type of taxes or fees or does not settle the taxes, fees, custom fees or the currency exchange in the same way as the legislation of the issuing

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article. 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party. 7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure	Member State does. **(3)** (Amend. – SG 49/10) Double criminality shall not be required for the following offences, if in the issuing State they carry maximum term of not less than three years of imprisonment or with another more severe penalty, or for them a measure requiring detention for a maximum term of not less than of 3 years is provided: 1. Participation in a criminal organisation, 2. Terrorism, 3. Trafficking in human beings, 4. Sexual exploitation of children and child pornography, 5. Illicit trafficking in narcotic drugs and psychotropic substances, 6. Illicit trafficking in weapons, munitions and explosives, 7. Corruption, 156 8. fraud, including that affecting the financial interests of the European Communities within the meaning of the Convention of 26 July 1995 on the protection of the European Communities' financial interests, 9. Laundering of the proceeds of offence, 10. Counterfeiting currency, including of the euro, 11. computer-related offence, 12. Environmental offence, including illicit trafficking in endangered animal species and in endangered plant species and varieties, 13. Facilitation of unauthorised entry and residence, 14. murder, grievous bodily injury, 15. illicit trade in human organs and tissue, 16. kidnapping, illegal restraint and hostage-taking, 17. racism and xenophobia, 18. organised or armed robbery, 19. illicit trafficking in cultural goods, including antiques and works of art, 20. swindling, 21. racketeering and extortion, 22. counterfeiting and piracy of products, 23. forgery of administrative documents and trafficking therein, 24. forgery of means of payment,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	25. illicit trafficking in hormonal substances and other growth promoters, 26. illicit trafficking in nuclear or radioactive materials, 27. trafficking in stolen vehicles, 28. rape, 29. arson, 30. offences within the jurisdiction of the International Criminal Court, 31. unlawful seizure of aircraft/ships, 32. sabotage **Criminal Procedure Code** **Article 471 Grounds and contents of international legal assistance** (1) International legal assistance in criminal matters shall be rendered to another state under the provisions of an international treaty executed to this effect, to which the Republic of Bulgaria is a party, or based on the principle of reciprocity. International legal assistance in criminal cases shall also be made available to international courts whose jurisdiction has been recognised by the Republic of Bulgaria. (2) International legal assistance shall comprise the following: 1. Service of process; 2. Acts of investigation; 3. Collection of evidence; 4. Provision of information; 5. Other forms of legal assistance, where they have been provided for in an international agreement to which the Republic of Bulgaria is a party or have been imposed on the basis of reciprocity.
Article 25 – General principles relating to mutual assistance 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35. 3 Each Party may, in urgent circumstances, make requests for mutual	**Criminal Procedure Code** **Article 471 Grounds and contents of international legal assistance** (1) International legal assistance in criminal matters shall be rendered to another state under the provisions of an international treaty executed to this effect, to which the Republic of Bulgaria is a party, or based on the principle of reciprocity. International legal assistance in criminal cases shall also be made available to international courts whose jurisdiction has been recognised by the Republic of Bulgaria.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.	(2) International legal assistance shall comprise the following: 1. Service of process; 2. Acts of investigation; 3. Collection of evidence; 4. Provision of information; 5. Other forms of legal assistance, where they have been provided for in an international agreement to which the Republic of Bulgaria is a party or have been imposed on the basis of reciprocity.
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	**Section III "A" from MINISTRY OF INTERIOR ACT - „Exchange of Information or Data with the Competent Bodies of the European Union Member States for Prevention, Discovery and Investigation of Crimes (new – SG 93/09, in force from 24.11.2009).** **Art. 161a. (new – SG 93/09, in force from 24.11.2009)** (1) Following the provisions of this section the MI through a competent specialized structure shall carry out a simplified exchange of information or data with the competent law enforcement administrations of the European Union Member States, and with the states signatories to the Schengen Agreement for prevention, discovery and investigation of crimes. (2) The Ministry of Interior through a competent specialized structure may

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	provide: 1. Information and data from the Ministry information funds; 2. Information or data, received from other state bodies or local government authorities, from legal entities and natural persons. (3) Exchange of information or data with the competent bodies of the European Union Member States and of the states signatories to the Schengen Agreement shall be done subject to observance of th, to which the Republic of Bulgaria is a party, and also subject to observance of the provisions of the Protection of Classified Information Act and the Protection of Personal Data Act. **Art. 161c. (new – SG 93/09, in force from 24.11.2009)** **(1)** Provision of the required information or data may be withdrawn where there are sufficient grounds to reckon that there is danger of: 1. Establishment of conditions threatening national security and public order; 2. Hindering actions of investigation or gathering data for initiation of penal proceedings; 3. Endangering a natural person's safety. **(2)** In addition to the cases under par. 1 provision of required information or data may be refused where they: 1. do not correspond to the objectives, for which they have been requested; 2. are related to a crime, for which the law provides a penalty of imprisonment for a period of up to one year or another less grave penalty. **(3)** The requested information or data shall be provided only if permission by the competent judicial body for access to them has been obtained. **Conditions** **Art. 161e. (new – SG 93/09, in force from 24.11.2009)** (1) Information or data shall be provided on the grounds of a request by the respective competent body of the Member State. (2) The request for provision of information or data shall be prepared in one of the official languages of the European Union and shall contain: 1. the justifications, that the respective information of data are available; 2. the purpose for which the information or data are requested;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	3. the connection between the purpose and the person, to which the information or data relate. (3) Information or data, required for prevention, discovery or investigation of crimes under Art. 36 of the Extradition and European Arrest Warrant Act, may be provided without addressing a request. **The Electronic communications act** – **Article 251Conditions**: – the request should come from competent authority; – the grounds that the information or data is available in Bulgaria; – purpose of the requested data; – what data exactly is needed (subscriber, traffic, etc.); – period of time for the data (if applicable – traffic data, etc.); – data is presented to asking party after a court approval (court order issued for the providers)
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each	**Criminal Procedure Code** Article 471 Grounds and contents of international legal assistance (1) International legal assistance in criminal matters shall be rendered to another state under the provisions of an international treaty executed to this effect, to which the Republic of Bulgaria is a party, or based on the principle of reciprocity. International legal assistance in criminal cases shall also be made available to international courts whose jurisdiction has been recognised by the Republic of Bulgaria. (2) International legal assistance shall comprise the following: 1. Service of process; 2. Acts of investigation; 3. Collection of evidence; 4. Provision of information; 5. Other forms of legal assistance, where they have been provided for in an international agreement to which the Republic of Bulgaria is a party or have been imposed on the basis of reciprocity. Article 472 Refusal of international legal assistance

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Party shall ensure that the details held on the register are correct at all times. 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party. 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities. 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary. 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly. 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party. b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol). c Where a request is made pursuant to sub-paragraph a. of this article	International legal assistance may be refused if the implementation of the request could threaten the sovereignty, the national security, the public order and other interests, protected by law. Article 473 Appearance of witnesses and experts before a foreign national court (1) Appearance of witnesses and experts before foreign national judicial bodies shall be allowed only if assurance is provided, that the individuals summonsed, regardless of their citizenship, shall not incur criminal liability for acts committed prior to summonsing. In the event they refuse to appear, no coercive measures may be taken in respect thereof. (2) The surrender of individuals remanded in custody to the purpose of being interrogated as witnesses or experts shall be only admitted under exceptional circumstances at the discretion of a panel of the respective district court, based on papers submitted by the other country, or an international court, provided the individual consents to being surrendered, and his/her stay in another state does not extend beyond the term of his/her remand in custody. Article 474 Interrogation of individuals through a video or phone conference (1) The judicial body of another state may conduct the interrogation, through a video or phone conference, of an individual who appears as a witness or expert in the criminal proceedings and is in the Republic of Bulgaria, where so envisaged in an in international agreement to which the Republic of Bulgaria is a party. An interrogation through a video conference involving the accused party or a suspect may only be conducted upon their consent and once the participating Bulgarian judicial authorities and the judicial authorities of the other state agree on the manner in which the video conference will be conducted. An interrogation through a video or phone conference may only be conducted where this does not stand in contradiction to fundamental principles of Bulgarian law. (2) The request for interrogation filed by a judicial body of the other state should indicate: 1. The reason why the appearance in person of the individual is undesirable or impossible; 2. The name of the judicial body of the other state; 3. The data of individuals who shall conduct the interrogation; 4. The consent of the individual who shall be interrogated as a witness or expert through a phone conference;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	5. Consent of the accused party who will take part in an interrogation hearing through a video conference. (3) Bulgarian competent authorities in the field of criminal proceedings shall implement requests for interrogation through a video or phone conferences. A request for interrogation through a video or phone conference shall be implemented for the needs of pre-trial proceedings by the National Investigation Service. For the need of judicial proceedings, a request for interrogation through a phone conference shall be implemented by a court of equal standing at the place of residence of the individual, and for interrogation through a video conference - by the Appellate Court at the place of residence of the individual. The competent Bulgarian authority may require the requesting party to ensure technical facilities for interrogation. (4) The interrogation shall be directly conducted by the judicial authority of the requesting state or under its direction, in compliance with the legislation thereof. (5) Prior to the interrogation the competent Bulgarian authority shall ascertain the identity of the person who needs to be interrogated. Following the interrogation a record shall be drafted, which shall indicate: 1. The date and location thereof; 2. The data of the interrogated individual and his or her consent, if it is required; 3. The data of individuals who took part therein on the Bulgarian side; 4. The implementation of other conditions accepted by the Bulgarian party. (6) An individual who is abroad may be interrogated by a competent Bulgarian authority or under its direction through a video or phone conference where the legislation of said other state so admits. The interrogation shall be conducted in compliance with Bulgarian legislation and the provisions of international agreements to which the Republic of Bulgaria is a party, wherein the above means of interrogation have been regulated. (7) The interrogation through a video or phone conference under para 6 shall be carried out in respect of pre-trial proceedings by the National Investigation Service, whereas in respect of trial proceedings - by the court. (8) The provisions of paras 1 - 5 shall apply mutatis mutandis to the interrogation of individuals under para 6. Article 475 Procedure for submission of a request to another country or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	international court (1) A letter rogatory for international legal assistance shall contain data about: the body filing the letter; the subject and the reasoning of the letter; full name and citizenship of the individual to whom the letter refers; name and address of the individual on whom papers are to be served; and, where necessary - the indictment and a brief description of the relevant facts. (2) A letter rogatory for international legal assistance shall be forwarded to the Ministry of Justice, unless another procedure is provided by international treaty to which the Republic of Bulgaria is a party. Article 476 Execution of request by another country or international court (1) Request for international legal assistance shall be executed pursuant to the procedure provided by Bulgaria law or pursuant to a procedure provided by an international agreement to which the Republic of Bulgaria is a part. A request may also be implemented pursuant to a procedure provided for in the law of the other country or the statute of the international court, should that be requested and if it is not contradictory to the Bulgarian law. The other country or international court shall be notified of the time and place of execution of the request, should that be requested. (2) Request for legal assistance and all other communications from the competent authorities of another state which are sent and received by fax or e-mail shall be admitted and implemented by the competent Bulgarian authorities pursuant to the same procedure as those sent by ordinary mail. The Bulgarian authorities shall be able to request the certification of authenticity of the materials sent, as well as to obtain originals by express mail. (3) The Supreme Prosecution Office of Cassation shall set up, together with other states, joint investigation teams, in which Bulgarian prosecutors and investigative bodies will take part. An agreement with the competent authorities of the participant states shall be entered in respect of the activities, duration and composition of a joint investigation team. The joint investigation team shall comply with provisions of international agreements, the stipulations of the above agreement and Bulgarian legislation while being on the territory of the Republic of Bulgaria. (4) The Supreme Prosecution Office of Cassation shall file requests with other states for investigation through an under-cover agent, controlled deliveries and cross-border observations and it shall rule on such requests by other states.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(5) In presence of mutuality a foreign authority carrying out investigation through an agent under cover on the territory of the Republic of Bulgaria shall be able to collect evidence in accordance with its national legislation. (6) In urgent cases involving the crossing of the state border for the purposes of cross-border observations on the territory of the Republic of Bulgaria the Supreme Prosecution Office of Cassation shall be immediately notified. It shall make a decision to proceed with or terminate cross-border observations pursuant to the terms and conditions of the Special Intelligence Means Act . (7) The implementation of requests for controlled delivery or cross-border observations filed by other states shall be carried out by the competent investigation authority. It shall be able to request assistance from police, customs and other administrative bodies. Article 477 Costs for execution of request The costs for execution of request shall be distributed between the countries in compliance with international treaties to which the Republic of Bulgaria is a party, or on the basis of the principle of reciprocity. MLA authority: Ministry of Justice (trial stage), Supreme Cassation Prosecutor's Office (pre-trial stage), Ministry of Justice (extradition), Supreme Cassation Prosecutor's Office (provisional arrests)
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	See previous

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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	Preservation orders are possible under the broad powers defined in Article 159 of the Criminal Procedure Code which obliges legal and physical persons to "preserve and hand over" computerized data, including traffic data and other objects that may be of significance to the case. This is ordered by a court or, during pre-trial proceedings, by a prosecutor or the police. It pertains to all types of data, any crime and any legal or physical person In addition, search and seizure powers may be used. Moreover, data retention is regulated in the Bulgarian Electronic Communication Act. The powers used for expedited preservation at the domestic level can also be applied for international requests. A 24/7 contact point has been established at the Cybercrime Section, General Directorate for Combating Organized Crime, Ministry of the Interior. **Criminal Procedure Code** Article 159 Obligation to hand over objects, papers, computerised data, data about subscribers to computer information service and traffic data Upon request of the court or the bodies of pre-trial proceedings, all institutions, legal persons, officials and citizens shall be obligated to preserve and hand over all objects, papers, computerized data, including traffic data, that may be of significance to the case.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
disclosure the condition of dual criminality cannot be fulfilled. 5 In addition, a request for preservation may only be refused if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 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.	Preservation and partial disclosure orders are possible under the broad powers defined in Article 159 of the Criminal Procedure Code which obliges legal and physical persons to "preserve and hand over" computerized data, including traffic data and other objects that may be of significance to the case. Traffic data is also retained under data retention regulations. Regarding international requests (Article 30 Budapest Convention): There are no special provisions for partial disclosure for domestic or international purposes. For international requests Bulgaria uses general provisions to obtain the full disclosure at the domestic level but discloses to foreign authorities only the partial information needed. A formal MLA request is not necessary. **Criminal Procedure Code** Article 159 Obligation to hand over objects, papers, computerised data, data about subscribers to computer information service and traffic data Upon request of the court or the bodies of pre-trial proceedings, all institutions, legal persons, officials and citizens shall be obligated to preserve and hand over

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	all objects, papers, computerized data, including traffic data that may be of significance to the case.
Article 31 – Mutual assistance regarding accessing of stored computer data 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where: 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.	General principles apply.
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.	No legal regulations
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.	See general provisions regarding real-time collection of data

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	See general provisions regarding real-time collection of data
Article 35 – 24/7 Network 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects. 2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis. 3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.	**General Directorate for Combating Organised Crime, Ministry of the Interior** **Description of 24/7 contact point:** 24/7 Contact Point is located in the Cybercrime Section within General Directorate for Combating Organised Crime. The Cybercrime Section has nationwide responsibility for all IT or computer related investigations. The Cybercrime Section aims to provide the requesting countries with useful investigative information. Assistance will be provided to the requesting country as soon as possible. The personnel receiving the requests for assistance will also be available by e-mail. **Spoken languages of the 24/7 contact point:** Bulgarian, English, Russian, French, Spanish, Portuguese **Information to be provided:** when calling the 24/7 contact point's number in order to facilitate the processing of requests: Identify yourself, your agency and the country that you represent. Send your request by fax or by e-mail. If calling, ask to be connected to the persons above. Time zone: UTC/GMT+ 3 hours
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,	**Reservation contained in the instrument of ratification deposited on 7 April 2005 – Or. Engl.** In accordance with Article 14, paragraph 3, of the Convention, the Republic of Bulgaria reserves the right to apply the measures referred to in Article 20 only

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	to serious offences, as they are defined by the Bulgarian Criminal Code. **Period covered: 01/08/2005 -** Articles concerned : 14

Back to the Table of Contents