# Switzerland

## Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

## Table of contents

*Version 01 May 2020*

[reference to the provisions of the Budapest Convention]



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



COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

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

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| **Chapter I – Use of terms** | |
| **Article 1 – "Computer system", "computer data", "service provider", "traffic data":**<br>For the purposes of this Convention:<br>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;<br><br>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;<br>c "service provider" means:<br><br>i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and<br>ii any other entity that processes or stores computer data on behalf of such communication service or users of such service;<br>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 | |
| **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**<br>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when | **Swiss Criminal Code** |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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. | **Art. 143bis. Offences against property / Unauthorised access to a data processing system**<br>**Unauthorised access to a data processing system**<br><br>1 Any person who obtains unauthorised access by means of data transmission equipment to a data processing system that has been specially secured to prevent his access is liable on complaint to a custodial sentence not exceeding three years or to a monetary penalty.<br><br>2 Any person who markets or makes accessible passwords, programs or other data that he knows or must assume are intended to be used to commit an offence under paragraph 1 is liable to a custodial sentence not exceeding three years or to a monetary penalty. |
| **Article 3 – Illegal interception**<br>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. | **Swiss Criminal Code**<br><br>**Art. 143 1. Offences against property / Unauthorised obtaining of data**<br>**Unauthorised obtaining of data**<br><br>1 Any person who for his own or for another's unlawful gain obtains for himself or another data that is stored or transmitted electronically or in some similar manner and which is not intended for him and has been specially secured to prevent his access is liable to a custodial sentence not exceeding five years or to a monetary penalty.<br><br>2 The unauthorised obtaining of data to the detriment of a relative or family member is prosecuted only on complaint. |
| **Article 4 – Data interference**<br>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.<br>2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm. | **Swiss Criminal Code**<br><br>**Art. 144bis 1. Offences against property / Damage to data**<br>**Damage to data**<br><br>1. Any person who without authority alters, deletes or renders unusable data that is stored or transmitted electronically or in some other similar way is liable on complaint to a custodial sentence not exceeding three years or to a monetary penalty. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | If the offender has caused major damage, a custodial sentence of from one to five years may be imposed. The offence is prosecuted ex officio.<br><br>2. Any person who manufactures, imports, markets, advertises, offers or otherwise makes accessible programs that he knows or must assume will be used for the purposes described in paragraph 1 above, or provides instructions on the manufacture of such programs is liable to a custodial sentence not exceeding three years or to a monetary penalty.<br><br>If the offender acts for commercial gain, a custodial sentence of from one to five years may be imposed. |
| **Article 5 – System interference**<br>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 | |
| **Article 6 – Misuse of devices**<br>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:<br>a the production, sale, procurement for use, import, distribution or otherwise making available of:<br>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;<br>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,<br>with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and<br><br>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. | **Swiss Criminal Code**<br><br>**Art. 144bis 1. Offences against property / Damage to data**<br>**Damage to data**<br><br>2. Any person who manufactures, imports, markets, advertises, offers or otherwise makes accessible programs that he knows or must assume will be used for the purposes described in paragraph 1 above, or provides instructions on the manufacture of such programs is liable to a custodial sentence not exceeding three years or to a monetary penalty.<br><br>If the offender acts for commercial gain, a custodial sentence of from one to five years may be imposed. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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.<br><br>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. | |
| **Title 2 – Computer-related offences** | |
| **Article 7 – Computer-related forgery**<br>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. | **Swiss Criminal Code**<br><br>**Art. 251[1] / Forgery of a document**<br>**Forgery of a document**<br><br>1. Any person who with a view to causing financial loss or damage to the rights of another or in order to obtain an unlawful advantage for himself or another,<br><br>produces a false document, falsifies a genuine document, uses the genuine signature or mark of another to produce a false document, falsely certifies or causes to be falsely certified a fact of legal significance or,<br><br>makes use of a false or falsified document in order to deceive,<br><br>is liable to a custodial sentence not exceeding five years or to a monetary penalty.<br><br>2. In particularly minor cases, a custodial sentence not exceeding three years or a monetary penalty may be imposed. |
| **Article 8 – Computer-related fraud**<br>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: | **Swiss Criminal Code**<br><br>**Art. 147 1. Offences against property / Computer fraud**<br>**Computer fraud** |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| a any input, alteration, deletion or suppression of computer data;<br><br>b any interference with the functioning of a computer system,<br><br>with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person. | 1 Any person who with a view to his own or another's unlawful gain, by the incorrect, incomplete or unauthorised use of data, or in a similar way, influences the electronic or similar processing or transmission of data and as a result causes the transfer of financial assets, thus occasioning loss to another, or immediately thereafter conceals such a transfer is liable to a custodial sentence not exceeding five years or to a monetary penalty.<br>2 If the offender acts for commercial gain, he is liable to a custodial sentence not exceeding ten years or to a monetary penalty of not less than 90 daily penalty units.<br>3 Computer fraud to the detriment of a relative or family member is prosecuted only on complaint. |
| **Title 3 – Content-related offences** | |
| **Article 9 – Offences related to child pornography**<br>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:<br>a producing child pornography for the purpose of its distribution through a computer system;<br>b offering or making available child pornography through a computer system;<br>c distributing or transmitting child pornography through a computer system;<br>d procuring child pornography through a computer system for oneself or for another person;<br>e possessing child pornography in a computer system or on a computer-data storage medium.<br><br>2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:<br>a a minor engaged in sexually explicit conduct;<br>b a person appearing to be a minor engaged in sexually explicit conduct;<br>c realistic images representing a minor engaged in sexually explicit conduct | **Swiss Criminal Code**<br><br>**Art. 197[1]4. Pornography**<br>**4. Pornography**<br><br>1 Any person who offers, shows, passes on or makes accessible to a person under the age of 16 pornographic documents, sound or visual recordings, depictions or other items of a similar nature or pornographic performances, or broadcasts any of the same on radio or television is liable to a custodial sentence not exceeding three years or to a monetary penalty.<br>2. Any person who exhibits in public items or performances as described in paragraph 1 above or shows or otherwise offers the same unsolicited to others is liable to a fine. Any person who, in advance, draws the attention of visitors to private exhibitions or performances to their pornographic character does not commit an offence.<br>3 Any person who recruits or causes a minor to participate in a pornographic performance is liable to a custodial sentence not exceeding three years or to a monetary penalty.<br>4 Any person who produces, imports, stores, markets, advertises, exhibits, offers, shows, passes on or makes accessible to others, acquires, or procures or possesses via electronic media or otherwise items or performances as described in paragraph 1 above that contain sexual acts involving animals, acts of violence involving adults or non-genuine sexual acts with minors is liable to a custodial |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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.<br><br>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. | sentence not exceeding three years or to a monetary penalty. If the items or performances contain genuine sexual acts with minors, the penalty is a custodial sentence not exceeding five years or a monetary penalty.<br>5 Any person who consumes or who for his or her own consumption produces, imports, stores, acquires or procures or possesses via electronic media or otherwise items or performances as described in paragraph 1 above that contain sexual acts involving animals, acts of violence involving adults or non-genuine sexual acts with minors is liable to a custodial sentence not exceeding one year or to a monetary penalty. If the items or performances contain genuine sexual acts with minors, the penalty is a custodial sentence not exceeding three years or a monetary penalty.<br>6 In the case offences under paragraphs 4 and 5, the items shall be forfeited.<br>7 If the offender acts for financial gain, the custodial sentence must be combined with a monetary penalty.<br>8 Minors over the age of 16 are not liable to any penalty if by mutual consent they produce items or performances as described in paragraph 1 above that involve each other, or possess or consume such items or performances.<br>9 Items or recordings as described in paragraphs 1–5 above are not regarded as pornographic if they have a cultural or scientific value that justifies their protection by law. |
| **Title 4 – Offences related to infringements of copyright and related rights** | |
| **Article 10 – Offences related to infringements of copyright and related rights**<br>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.<br>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 | **Federal Act on Copyright and Related Rights**<br><br>Art. 67 **Copyright infringement**<br>[1] On the complaint of the person whose rights have been infringed, any person who wilfully and unlawfully commits any of the following acts is liable to a custodial sentence not exceeding one year or a monetary penalty:<br><br>a. uses a work under a false designation or a designation that differs from that decided by the author;<br>b. publishes a work;<br>c.modifies a work;<br>d. uses a work to create a derivative work;<br>e. produces copies of a work in any manner;<br>f. offers, transfers or otherwise distributes copies of a work; |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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.<br>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. | g. recites, performs or presents a work or makes a work perceptible somewhere else either directly or with the help of any kind of medium;<br>g$^{bis}$.[2] makes a work available through any kind of medium in such a way that persons may access it from a place and at a time individually chosen by them;<br>h. broadcasts a work by radio, television or similar means, including by wire, or retransmits a broadcast work by means of technical equipment, the operator of which is not the original broadcasting organisation;<br>i.[3] makes a work made available, a broadcast work or a retransmitted work perceptible;<br>k.[4] refuses to notify the authority concerned of the origin and quantity of items in his possession that have been unlawfully manufactured or placed on the market, and to name the recipients and disclose the extent of any distribution to commercial and industrial consumers;<br><br>rents out a computer program.<br><br>[2] Any person who has committed any act mentioned in paragraph 1 for commercial gain shall be prosecuted ex officio. The penalty is a custodial sentence not exceeding five years or a monetary penalty. The custodial sentence must be combined with a monetary penalty.[5]<br><br>Art. 68 **Omission of source**<br>Any person who intentionally omits to indicate the source used where required by statute (Articles 25 and 28) and where the author is named therein, to provide the name of the author, is liable to a fine on the complaint of the person whose rights have been infringed.<br><br>Art. 69 **Infringement of related rights**<br>[1] On the complaint of the person whose rights have been infringed, any person who wilfully and unlawfully commits any of the following acts is liable to a custodial sentence not exceeding one year or a monetary penalty:[1]<br><br>a. broadcasts the performance of a work by radio, television or similar means, including by wire;<br>b. fixes a performance of a work on blank media;<br>c. offers, transfers or otherwise distributes copies of a performance of a work; |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | d. retransmits a broadcast performance of a work by means of technical equipment, the operator of which is not the original broadcasting organisation;<br>e.[2] makes a performance of a work made available, a broadcast performance of a work or a retransmitted performance of a work perceptible;<br>e$^{bis}$.[3] uses a performance of a work under a false name or under a name other than the artist name designated by the performer;<br>e$^{ter}$.[4] makes a performance of a work, a phonogram or audio-visual fixation or a broadcast available through any kind of medium in such a way that persons may access them from a place and at a time individually chosen by them;<br>f. reproduces a phonogram or audio-visual fixation and offers, transfers or otherwise distributes the reproductions;<br>g. retransmits a broadcast;<br>h. fixes a broadcast on blank media;<br><br>reproduces a broadcast fixed on blank media or distributes copies of such reproductions;<br><br>refuses to notify the responsible authority concerned of the origin and quantity of the carriers of a performance protected under Articles 33, 36 or 37 in his possession that have been unlawfully manufactured or placed on the market, or to name the recipients and disclose the extent of any distribution to commercial and industrial customers.<br>[2] Any person who has committed any act mentioned in paragraph 1 for commercial gain shall be prosecuted ex officio. The penalty is a custodial sentence not exceeding five years or a monetary penalty. The custodial sentence must be combined with a monetary penalty.[6] |

Back to the Table of Contents

| | |
|---|---|
| | Art. 69**a**[1] **Offences relating to technical protection measures and to rights- management information**<br>[1] On the complaint of the person whose protection has been violated, any person who wilfully and unlawfully commits any of the following acts is liable to a monetary penalty:<br>a. circumvents effective technological measures under Article 39 paragraph 2 with the intention of illegally using works or other protected subject-matter;<br>b. manufactures, imports, offers, transfers or otherwise distributes, rents, gives or advertises for use, or possesses for commercial purposes devices, products or components, or provides services which:<br>1. are the subject-matter of sales promotion, advertising or marketing with the goal of circumventing effective technological measures,<br>2. have only a limited commercially significant purpose or use other than the circumvention of effective technological measures, or<br>3. are primarily designed, manufactured, adapted or performed for the purpose of enabling or facilitating the circumvention of effective technological measures;<br>c. removes or alters electronic rights management information on copyright and related rights under Article 39c paragraph 2;<br>d. reproduces, imports, offers, transfers or otherwise distributes, broadcasts or makes perceptible or available works or other protected subject-matter on which electronic rights management information under Articles 39c paragraph 2 have been removed or altered.<br>[2] Any person who has committed any act mentioned in paragraph 1 for commercial gain shall be prosecuted ex officio. The penalty is a custodial sentence not exceeding one year or a monetary penalty. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | [3] Acts under paragraph 1 letter c and d are only liable to prosecution where they are carried out by a person who is known or, under the circumstances, should be known, for instigating, enabling, facilitating or concealing infringements of copyright or related rights. |
| **Title 5 – Ancillary liability and sanctions** | |
| **Article 11 – Attempt and aiding or abetting**<br>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.<br>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.<br>3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article. | **Swiss Criminal Code**<br><br>**Art. 22 4. Attempts / Criminal liability for attempts**<br>**4. Attempts**<br><br>Criminal liability for attempts<br><br>1 If, having embarked on committing a felony or misdemeanour, the offender does not complete the criminal act or if the result required to complete the act is not or cannot be achieved, the court may reduce the penalty.<br><br>2 If the offender fails to recognise through a serious lack of judgement that the act cannot under any circumstances be completed due to the nature of the objective or the means used to achieve it, no penalty is imposed.<br><br>**Art. 24 5. Participation / Incitement**<br>**5. Participation**<br><br>Incitement<br><br>1 Any person who has wilfully incited another to commit a felony or a misdemeanour, provided the offence is committed, incurs the same penalty as applies to the person who has committed the offence.<br><br>2 Any person who attempts to incite someone to commit a felony incurs the penalty applicable to an attempt to commit that felony.<br><br>**Art. 25 5. Participation / Complicity**<br>**Complicity** |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | Any person who wilfully assists another to commit a felony or a misdemeanour is liable to a reduced penalty. |
| **Article 12 – Corporate liability**<br>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:<br>a a power of representation of the legal person;<br>b an authority to take decisions on behalf of the legal person;<br>c an authority to exercise control within the legal person.<br>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.<br>3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.<br>4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence. | **Swiss Criminal Code**<br><br>**Title Seven: Corporate Criminal Liability**<br>**Art. 102 Liability under the criminal law**<br>**Liability under the criminal law**<br><br>1 If a felony or misdemeanour is committed in an undertaking in the exercise of commercial activities in accordance with the objects of the undertaking and if it is not possible to attribute this act to any specific natural person due to the inadequate organisation of the undertaking, then the felony or misdemeanour is attributed to the undertaking. In such cases, the undertaking is liable to a fine not exceeding 5 million francs.<br><br>2 If the offence committed falls under Articles 260ter, 260quinquies, 305bis, 322ter, 322quinquies, 322septies paragraph 1 or 322octies, the undertaking is penalised irrespective of the criminal liability of any natural persons, provided the undertaking has failed to take all the reasonable organisational measures that are required in order to prevent such an offence.1<br><br>3 The court assesses the fine in particular in accordance with the seriousness of the offence, the seriousness of the organisational inadequacies and of the loss or damage caused, and based on the economic ability of the undertaking to pay the fine.<br><br>4 Undertakings within the meaning of this title are:<br><br>a. any legal entity under private law;<br>b. any legal entity under public law with exception of local authorities;<br>c. companies;<br>d. sole proprietorships. |
| **Article 13 – Sanctions and measures**<br>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.<br>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. | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | |
| ***Section 2 – Procedural law*** | |
| **Article 14 – Scope of procedural provisions**<br>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.<br>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:<br>a the criminal offences established in accordance with Articles 2 through 11 of this Convention;<br>b other criminal offences committed by means of a computer system; and<br>c the collection of evidence in electronic form of a criminal offence.<br>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.<br>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:<br>i is being operated for the benefit of a closed group of users, and<br>ii does not employ public communications networks and is not connected with another computer system, whether public or private,<br>that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21 | |
| **Article 15 – Conditions and safeguards** | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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.<br>2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.<br><br>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. | |
| **Article 16 – Expedited preservation of stored computer data**<br>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.<br><br>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.<br><br>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 | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.<br><br>4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. | |
| **Article 17 – Expedited preservation and partial disclosure of traffic data**<br>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:<br>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<br>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.<br><br>2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. | |
| **Article 18 – Production order**<br>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:<br>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<br>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.<br><br>2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.<br>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 | **Swiss Criminal Procedure Code**<br><br>Art. 273 Subscriber information, location identification and technical transmission features<br>1 If there is a strong suspicion that a felony or misdemeanour or a contravention in terms of Article 179septies SCC has been committed, and if the requirements of Article 269 paragraph 1 letters b and c of this Code are met, the public prosecutor may request metadata relating to telecommunications in accordance with Article 8 letter b of the Federal Act of 18 March 2016 on the Surveillance of Postal and Telecommunications Traffic (SPTA) and metadata relating to post in accordance with Article 19 paragraph 1 letter b SPTA relating to the person under surveillance.<br><br>2 The order requires the approval of the compulsory measures court. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:<br>a the type of communication service used, the technical provisions taken thereto and the period of service;<br>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;<br>c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement. | 3 The information mentioned in paragraph 1 may be requested irrespective of the duration of surveillance and for the 6 months prior to the date of the request. |
| **Article 19 – Search and seizure of stored computer data**<br>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:<br>a a computer system or part of it and computer data stored therein; and<br>b a computer-data storage medium in which computer data may be stored<br>in its territory.<br>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.<br>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:<br>a seize or similarly secure a computer system or part of it or a computer-data storage medium;<br>b make and retain a copy of those computer data;<br>c maintain the integrity of the relevant stored computer data;<br>d render inaccessible or remove those computer data in the accessed computer system. | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.<br>5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. | |
| **Article 20 – Real-time collection of traffic data**<br>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:<br>a collect or record through the application of technical means on the territory of that Party, and<br>b compel a service provider, within its existing technical capability:<br>i to collect or record through the application of technical means on the territory of that Party; or<br>ii to co-operate and assist the competent authorities in the collection or recording of,<br>traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.<br>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.<br>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.<br>4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. | **Swiss Criminal Procedure Code**<br><br>**Art. 269bis Use of special technical devices for the surveillance of telecommunications**<br>1 The public prosecutor may order the use of special technical devices for the surveillance of telecommunications in order to listen to or record conversations, identify a person or property or determine their location if:<br><br>a.<br>the requirements of Article 269 are met;<br>b.<br>previous telecommunications surveillance measures under Article 269 have been unsuccessful or surveillance with these measures would be futile or disproportionately difficult;<br>c.<br>the authorisation required under telecommunications law has been obtained to use these devices at the time of use.<br>2 The public prosecutor shall keep statistics on the use of these forms of surveillance. The Federal Council shall regulate the details.<br><br>**Art. 269ter Use of special software for the surveillance of telecommunications**<br>1 The public prosecutor may order the introduction of special software into a data processing system in order to intercept and recover the content of communications and telecommunications metadata in unencrypted form provided: |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | a.<br>the conditions of Article 269 paragraphs 1 and 3 are met;<br>b.<br>the proceedings relate to an offence listed in Article 286 paragraph 2;<br>c.<br>previous telecommunications surveillance measures under Article 269 have been unsuccessful or surveillance with these measures would be futile or disproportionately difficult.<br>2 In the surveillance order, the public prosecutor shall specify:<br><br>a.<br>the desired data types; and<br>b.<br>the non-public spaces that may have to be entered in order to introduce special software into the relevant data processing system.<br>3 Data not covered by paragraph that is collected when using such software must be destroyed immediately. No use may be made of information obtained from such data.<br><br>4 The public prosecutor shall keep statistics on these forms of surveillance. The Federal Council shall regulate the details.<br><br>**Art. 269quater Requirements applicable to special software for the surveillance of telecommunications**<br>1 The only special software that may be used is that which records the surveillance unalterably and without interruption. The record forms part of the case files.<br><br>2 The recovery of data from the data processing system under surveillance to the relevant criminal justice authority must take place securely.<br><br>3 The criminal justice authority shall ensure that the source code can be checked in order to verify that the software has only legally permitted functions. |
| **Article 21 – Interception of content data** | **Swiss Criminal Procedure Code** |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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:<br>a collect or record through the application of technical means on the territory of that Party, and<br>b compel a service provider, within its existing technical capability:<br>i to collect or record through the application of technical means on the territory of that Party, or<br>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.<br>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.<br>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.<br>4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. | **Art. 269bis Use of special technical devices for the surveillance of telecommunications**<br>1 The public prosecutor may order the use of special technical devices for the surveillance of telecommunications in order to listen to or record conversations, identify a person or property or determine their location if:<br><br>a.<br>the requirements of Article 269 are met;<br>b.<br>previous telecommunications surveillance measures under Article 269 have been unsuccessful or surveillance with these measures would be futile or disproportionately difficult;<br>c.<br>the authorisation required under telecommunications law has been obtained to use these devices at the time of use.<br>2 The public prosecutor shall keep statistics on the use of these forms of surveillance. The Federal Council shall regulate the details.<br><br>**Art. 269ter Use of special software for the surveillance of telecommunications**<br>1 The public prosecutor may order the introduction of special software into a data processing system in order to intercept and recover the content of communications and telecommunications metadata in unencrypted form provided:<br><br>a.<br>the conditions of Article 269 paragraphs 1 and 3 are met;<br>b.<br>the proceedings relate to an offence listed in Article 286 paragraph 2;<br>c.<br>previous telecommunications surveillance measures under Article 269 have been unsuccessful or surveillance with these measures would be futile or disproportionately difficult.<br>2 In the surveillance order, the public prosecutor shall specify:<br><br>a.<br>the desired data types; and |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | b.<br>the non-public spaces that may have to be entered in order to introduce special software into the relevant data processing system.<br>3 Data not covered by paragraph that is collected when using such software must be destroyed immediately. No use may be made of information obtained from such data.<br><br>4 The public prosecutor shall keep statistics on these forms of surveillance. The Federal Council shall regulate the details.<br><br>**Art. 269quater Requirements applicable to special software for the surveillance of telecommunications**<br>1 The only special software that may be used is that which records the surveillance unalterably and without interruption. The record forms part of the case files.<br><br>2 The recovery of data from the data processing system under surveillance to the relevant criminal justice authority must take place securely.<br><br>3 The criminal justice authority shall ensure that the source code can be checked in order to verify that the software has only legally permitted functions. |
| ***Section 3 – Jurisdiction*** | |
| **Article 22 – Jurisdiction**<br>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:<br>a in its territory; or<br>b on board a ship flying the flag of that Party; or<br>c on board an aircraft registered under the laws of that Party; or<br>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.<br>2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. | Application of the Penal Code of the Republic of Slovenia to Any Person Who Commits a Criminal Offence in Its Territory<br><br>**Criminal Procedure Code, Article 10-14**<br><br>(1) The Penal Code of the Republic of Slovenia shall apply to any person who commits a criminal offence in the territory of the Republic of Slovenia.<br>(2) The Penal Code of the Republic of Slovenia shall also apply to any person who commits a criminal offence on a domestic vessel regardless of its location at the time of the committing of the offence.<br>(3) The Penal Code of the Republic of Slovenia shall also apply to any person who commits a criminal offence on a domestic civil aircraft in flight or on a domestic military aircraft regardless of its location at the time of the committing of the offence. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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.<br>4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.<br>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. | Application of the Penal Code of the Republic of Slovenia for Specific Criminal Offences Committed in a Foreign Country Article 11<br>The Penal Code of the Republic of Slovenia shall apply to any person who, in a foreign country, commits<br>- a criminal offence under Article 243 of this Penal Code or the criminal offences referred to in Articles 332, 333 and 334 of this Code, provided that they were committed in the ecological protection zone or in the continental shelf of the Republic of Slovenia;<br>- criminal offences under Article 108 and Articles 348-360 of this Penal Code.<br><br>Application of the Penal Code of the Republic of Slovenia to Citizens of the Republic of Slovenia Who Commit a Criminal Offence Abroad<br>Article 12<br>The Penal Code of the Republic of Slovenia shall be applicable to any citizen of the Republic of Slovenia who commits any criminal offence abroad other than those specified in the preceding Article.<br><br>Application of the Penal Code of the Republic of Slovenia to Foreign Citizens Who Commit a Criminal Offence Abroad<br>Article 13<br>(1) The Penal Code of the Republic of Slovenia shall apply to any foreign citizen who has, in a foreign country, committed a criminal offence against the Republic of Slovenia or any of its citizens, even though the offences in question are not covered by Article 11 of this Penal Code.<br>(2) The Penal Code of the Republic of Slovenia shall also be applicable to any foreign citizen who has, in a foreign country, committed a criminal offence against a third country or any of its citizens if he has been apprehended in the territory of the Republic of Slovenia, and not extradited to the foreign country. In such cases, the court shall not impose a sentence on the perpetrator which is heavier than the sentence prescribed by the law of the country in which the offence was committed.<br><br>Special Conditions for Prosecution<br>Article 14<br>(1) If, in cases under Article 10 and indent 1 of Article 11 of this Penal Code, the criminal procedure has been initiated or discontinued in a foreign country, the perpetrator may be prosecuted in the Republic of Slovenia only by permission of the Minister for Justice (hereinafter .the Minister.) with notice of the conditions under which the prosecution shall not violate the double jeopardy. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | (2) In cases under Articles 12 and 13 of this Penal Code, the perpetrator shall not be prosecuted:<br>1) if he has served the sentence imposed on him in the foreign country or if it was decided in accordance with an international agreement that the sentence imposed in the foreign country is to be served in the Republic of Slovenia;<br>2) if he has been acquitted by a foreign court or if his sentence has been remitted or the execution of the sentence has fallen under the statute of limitations;<br>3) if, according to foreign law, the criminal offence concerned may only be prosecuted upon the complaint of the injured party and the latter has not been filed.<br>(3) In cases under Articles 12 and 13, the perpetrator shall be prosecuted only insofar as his conduct constitutes a criminal offence in the country in which it was committed.<br>(4) If, in the case under Article 12 of this Penal Code, the criminal offence committed against the Republic of Slovenia or the citizen thereof does not constitute a criminal offence under the law of the country in which it was committed, the perpetrator of such an offence may be prosecuted only by permission of the Minister for Justice of the Republic of Slovenia.<br>(5) If, in all other cases except the cases referred to in indent 2 of Article 11 and paragraph 4 of this Article of this Penal Code, the criminal offence is not punished in the country in which it was committed, the perpetrator may be prosecuted only by permission of the Minister for Justice and with the proviso that, according to the general principles of law recognised by the international community, the offence in question constituted a criminal act at the time it was committed.<br>(6) In the case under Article 10, the prosecution of a foreign person may be transferred to another country under the conditions provided by the statute. |
| **Chapter III – International co-operation** | |
| **Article 24 – Extradition**<br>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.<br><br>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. | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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.<br>3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.<br>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.<br>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.<br>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.<br>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.<br><br>b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure | |
| **Article 25 – General principles relating to mutual assistance** | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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.<br><br>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.<br><br>3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.<br><br>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.<br><br>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. | |
| **Article 26 – Spontaneous information**<br>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 | **Federal Act on International Mutual Assistance in Criminal Matters**<br><br>**Art. 18b Electronic communications traffic data** |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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.<br><br>2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them. | 1 The federal or cantonal authority dealing with a request for mutual assistance may order the transmission of electronic communications traffic data to another State before conclusion of the mutual assistance proceedings if:<br>a. provisional measures indicate that the communication that is the subject of the request originated abroad; or<br>b. the data was acquired by the executing authority based on an order for authorised realtime surveillance (Art. 269–281 CrimPC55).<br>2 The data may not be used in evidence before the ruling on granting and the extent of mutual assistance is legally binding.<br>3 Notice of the ruling under paragraph 1 and any order or authorisation for surveillance must be given to the Federal Office immediately.<br><br>**Art. 67*a*** |
| **Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements**<br>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.<br>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.<br>b The central authorities shall communicate directly with each other;<br>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;<br>d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.<br>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. | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:<br>a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or<br>b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.<br>5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.<br>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.<br>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.<br>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.<br>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.<br>b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).<br>c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.<br>d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| authorities of the requesting Party to the competent authorities of the requested Party.<br>e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority. | |
| **Article 28 – Confidentiality and limitation on use**<br>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.<br>2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:<br>a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or<br>b not used for investigations or proceedings other than those stated in the request.<br>3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.<br>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**<br>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.<br>2 A request for preservation made under paragraph 1 shall specify:<br>a the authority seeking the preservation; | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;<br>c the stored computer data to be preserved and its relationship to the offence;<br>d any available information identifying the custodian of the stored computer data or the location of the computer system;<br>e the necessity of the preservation; and<br>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.<br>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.<br>4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.<br>5 In addition, a request for preservation may only be refused if:<br>a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or<br>b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.<br>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.<br>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 | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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**<br>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.<br>2 Disclosure of traffic data under paragraph 1 may only be withheld if:<br>a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or<br>b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. | **Art. 18b Electronic communications traffic data**<br>1 The federal or cantonal authority dealing with a request for mutual assistance may order the transmission of electronic communications traffic data to another State before conclusion of the mutual assistance proceedings if:<br>a. provisional measures indicate that the communication that is the subject of the request originated abroad; or<br>b. the data was acquired by the executing authority based on an order for authorised realtime surveillance (Art. 269–281 CrimPC55).<br>2 The data may not be used in evidence before the ruling on granting and the extent of mutual assistance is legally binding.<br>3 Notice of the ruling under paragraph 1 and any order or authorisation for surveillance must be given to the Federal Office immediately. |
| **Article 31 – Mutual assistance regarding accessing of stored computer data**<br>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.<br>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.<br>3 The request shall be responded to on an expedited basis where:<br>a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or<br>b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation. | |
| **Article 32 – Trans-border access to stored computer data with consent or where publicly available**<br>A Party may, without the authorisation of another Party: | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or<br>b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system. | |
| **Article 33 – Mutual assistance in the real-time collection of traffic data**<br>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.<br>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. | **Art. 18b Electronic communications traffic data**<br>1 The federal or cantonal authority dealing with a request for mutual assistance may order the transmission of electronic communications traffic data to another State before conclusion of the mutual assistance proceedings if:<br>a. provisional measures indicate that the communication that is the subject of the request originated abroad; or<br>b. the data was acquired by the executing authority based on an order for authorised realtime surveillance (Art. 269–281 CrimPC55).<br>2 The data may not be used in evidence before the ruling on granting and the extent of mutual assistance is legally binding.<br>3 Notice of the ruling under paragraph 1 and any order or authorisation for surveillance must be given to the Federal Office immediately. |
| **Article 34 – Mutual assistance regarding the interception of content data**<br>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. | |
| **Article 35 – 24/7 Network**<br>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:<br>a the provision of technical advice;<br>b the preservation of data pursuant to Articles 29 and 30; | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| c the collection of evidence, the provision of legal information, and locating of suspects.<br>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.<br><br>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.<br><br>3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network. | |
| **Article 42 – Reservations**<br>By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made. | |

Back to the Table of Contents