# Liechtenstein

## Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

*Version 27 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: | Liechtenstein |
|---|---|
| **Signature of the Budapest Convention:** | 17/11/2008 |
| **Ratification/accession:** | 27/01/2016 |

| 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 | The definitions set out in Article 1 of the Convention ("computer system", "computer data", "service provider", and "traffic data") are included in Liechtenstein law.<br><br>a. A legal definition of "computer system" was newly introduced in the Liechtenstein Criminal Code (§ 74(1)(8) Strafgesetzbuch, StGB) in accordance with the Council of Europe Convention on Cybercrime. This definition reads as follows: "computer system: both individual and connected devices serving automatic data processing".<br><br>b. While the Criminal Code does not contain an explicit definition of the term "computer data", it does set out a very broad definition of data (§ 74 (1)(8) and § 74 (1a)), covering all data referred to in Article 1(b) of this Convention. The definition includes both personal and non-personal data as well as programs.<br><br>c. The term "service provider" is defined in both the Liechtenstein Communications Act (Article 3(1)(2)) and the Liechtenstein E-Commerce Act (Article 3(1)(b)). According to these definitions, a service provider means anyone who commercially offers third parties an electronic communication service or who makes a service available to the information society. This may be a natural or legal person or any other entity with legal capacity.<br><br>d. The term "traffic data" is defined in the Liechtenstein Communications Act as "data processed for the purpose of the conveyance of a communication to an electronic communications network or for the billing thereof" (Article 3 (1)(46) of the Communications Act). |
| **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** | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| **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 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. | To implement Article 2, a new provision was introduced in the Criminal Code (§ 118a), criminalizing illegal access to a computer system. The provision was further amended in 2019 to cover every case of so called "Hacking activity".<br>Under this provision, it is illegal to gain access to a computer system (or part of a computer system), by overcoming specific security precautions in said system, with the purpose of (1) obtaining knowledge of personal data which violates confidentiality interests of the person concerned, or (2) with the purpose of inflicting a disadvantage upon another person by using data stored on the system or by using the computer system.<br>The offence may be punished with imprisonment of up to six months or with a fine of up to 360 daily rates. If the offence is committed as a member of a criminal group, the term of imprisonment may be up to three years. If the offence is committed with regard to a computer system which is an essential part of the critical infrastructure, the term of imprisonment may be up to two years. |
| **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. | Analogously to § 118a of the Criminal Code (as described under Article 2), the abusive interception of data is punishable (§ 119a). The offence may be punished with imprisonment of up to six months or with a fine of up to 360 daily rates. |
| **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. | § 126a StGB punishes authorized changing, deleting, or otherwise making unusable or suppressing of data that is not at the perpetrator's disposal or sole disposal. The sentence may be imprisonment of up to six months or more, up to five years, depending on the damage caused, or a fine of up to 360 daily rates.<br>If a person compromises a great number of computer systems by using a computer programme, a computer password, an access code or comparable data, which make it possible to access a computer system or a part thereof, provided that these instruments, because of their particular nature, have been evidently created or adapted for this purpose, the sentence may increase up to three years imprisonment. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | If the offence is committed as a member of a criminal group or compromises essential elements of the critical infrastructure, the term of imprisonment may be between six month and five years. |
| **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 | § 126b StGB punishes entering or transmitting of data resulting in serious interference with the functioning of a computer system. The same objective elements of the offence and the same sentences are applicable as in §126a StGB. |
| **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.<br><br>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 | To implement Article 6 of the Cybercrime Convention, § 126c StGB was introduced as a preparatory offence. According to §126c, it is illegal to manufacture, introduce, distribute, sell, or make available a computer program created or adapted to commit an offence set out in Articles 2 to 5 of the Cybercrime Convention. § 126c also covers devices comparable to a computer program, computer passwords, access codes, or comparable data allowing access to a computer system. § 126c(2) implements the requirements under Article 6(2) of the Cybercrime Convention. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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. | Under § 225a of the Criminal Code (Forgery of data), it is illegal to produce false databy entering, changing, deleting, or suppressing data, or falsify genuine data with the intent that the data be used in legal transactions to prove a right, a legal relationship or a fact. The sentence under § 225a is imprisonment of up to one year or with a fine of up to 720 daily rates. |
| **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:<br><br>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. | Under § 148a of the Criminal Code (fraudulent misuse of data processing), it is illegal to enter, change, delete, or suppress data with the aim of unjustly enriching oneself or of causing detriment to the assets of another person. Under this provision, it is also illegal to otherwise intervene in the flow of a processing procedure. The sentence of imprisonment depends on the magnitude of the harm and ranges from six months to ten years or with a fine of up to 360 daily rates. |
| **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: | 1. The key article for the comprehensive criminalization of conduct relating to child pornography is § 219 of the Criminal Code. That article makes it illegal to produce, obtain, possess, offer, procure, transfer, present, or make available pornographic depictions of a minor. This is tantamount to a compete prohibition |

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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<br><br>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. | on the circulation of pornographic depictions of minors. § 219(4) also makes it illegal to knowingly access a pornographic depiction of a minor with the help of information or communication technology. This means the viewing of such content is already subject to prosecution, even if nothing is saved on a data carrier.<br><br>2. The term "pornographic depiction of minors" is defined in detail in § 219(5) StGB. The broad definition of this term covers Article 9(2)(a) to (c) of the Cybercrime Convention.<br><br>3. § 219 refers to minors. According to § 74(1)(3) of the Criminal Code, any person who has not yet reached the age of eighteen is considered a minor in Liechtenstein. |
| **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 | With the revision of the Copyright Act in 1999, Liechtenstein met the legal conditions for becoming a State party to the following agreements:<br><br>- Berne Convention for the Protection of Literary and Artistic Works (revised on 24 July 1971 in Paris)<br><br>- Convention of 26 October 1961 for the Protection of Producers of Phonograms against Unauthorized Duplication of their Phonograms (Rome Convention) |

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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 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. | - Universal Copyright Convention (revised on 24 July 1971 in Paris)<br><br>In 2007, Liechtenstein also acceded to the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty (both of 20 December 1996).<br><br>The criminal provisions of the Copyright Act of 1999 are set out in Articles 61 to 69. Article 61 covers copyright violations, Article 62 the omission of source citations, Article 63 the violation of related protective rights, Article 63a the violation of the protection of technical measures and information for asserting rights, Article 64 the violation of rights pertaining to databases, Article 65 the unauthorized assertion of rights, Article 66 criminal responsibility, Article 67 confiscation in criminal proceedings, Article 68 forfeiture, and Article 69 criminal prosecution. The requirements set out in Article 10 of the Cybercrime Convention are thus fully met under Liechtenstein law. |
| **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. | 1. The Liechtenstein Criminal Code criminalizes participation in an offence in § 12 StGB (treatment of all participants as perpetrators).<br><br>2. Attempted offences are also punishable under § 15 StGB (criminal liabilityof attempt). |
| **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 | Under § 74a of the Criminal Code, legal persons may be held liable for offences under criminal law and supplementary criminal law. The criminal liability of legal persons has been in effect since 2011 and is governed by §§ 74a–74g StGB and §§ 357a–357g of the Code of Criminal Procedure (Strafprozessordnung, StPO). |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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. | Liechtenstein laws thus cover the obligations arising from Article 12 of the Cybercrime Convention. |
| **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. | 1. All offences set out in Articles 2 to 11 of the Cybercrime Convention are punishable under Liechtenstein law. Illegal access to a computer system (Article 2), illegal interception of data (Article 3), damage to data (Article 4), interference with the functioning of a computer system (Article 5), and misuse of computer programs or access data (Article 6) are punishable with imprisonment of up to six months or a fine of up to 360 daily rates. The penalty available for computer-related fraud (Article 8) is imprisonment of up to six months or a monetary penalty of up to 360 daily rates; if certain qualifying conditions are met, the penalty may be increased to imprisonment of one to ten years. If, depending on the offence, aggravating circumstances apply such as commitment of the offence as a member of a criminal group, or if the attack is directed to a computer system which is an essential part of the critical infrastructure, or if serious damage, or serious interference is inflicted upon a computer system, the penalty may likewise be increased. Forgery of data (Article 7) is punishable with imprisonment of up to one year. Pornographic depiction of a minor (Article 9) may, depending on the gravity of the offence, be punished with up to 3 or up to 10 years of imprisonment. The same penalties apply to attempts, aiding and abetting, and incitement (Article 11) as to a completed offence.<br><br>2. Thanks to the criminal liability of legal persons, legal persons are likewise subject to these penalties and measures. |

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 | 1 and 2. The preconditions for Article 14 of the Cybercrime Convention are set out in the Liechtenstein Code of Criminal Procedure (StPO). It should be noted that Liechtenstein law does not provide for any special treatment of computer-related offences or electronic evidence in this regard. |
| **Article 15 – Conditions and safeguards**<br>1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are | 1. Liechtenstein law on criminal procedure and communications safeguards fundamental rights. Liechtenstein joined the Council of Europe Convention of 4 November 1950 for the Protection of Human Rights and Fundamental Freedoms |

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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. | in 1982 and the International Covenant on Civil and Political Rights in 1999. Both international treaties entered into force for Liechtenstein in the year they were ratified.<br><br>2. Under § 103(1) and § 96 StPO, data resulting from surveillance of electronic communication may be transmitted only pursuant to a judicial order. Exceptions are provided to implement the special rules relating to Article 20 and 21 of the Cybercrime Convention. |
| **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 computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. | 1. According to the Liechtenstein Communications Act (Article 52a(2)), retained data must be stored such that they and all other associated required information can be forwarded immediately to the authorities responsible for carrying out the surveillance of an electronic communication. The data stored pursuant to a retention requirement must normally be surrendered only pursuant to a judicial ruling § 102a StPO).<br><br>2. In Liechtenstein, storage of data by service providers is governed by the Communications Act. According to Article 52a(1) of the Communications Act, providers are required to store retained data for the purpose of of investigating a crime or a misdemeanor pursuant to § 102a StPO. Under article 52a(1) of the Communications Act, this data must be stored for a period of six months from the time the communication process is terminated. Upon expiry of that time period, the data must be deleted within seven days.<br><br>3. Normally, the National Police is responsible for securing the data and forwarding it to the Court of Justice. Official secrecy ensures confidentiality of the data. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. | |
| **Article 17 – Expedited preservation and partial disclosure of traffic data**<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. | 1a. Article 3(1)(48a) of the Communications Act defines retained data as traffic, location and subscriber data generated or processed when a subscriber accesses a public communications network or for the billing thereof, including data of unsuccessful call attempts, where such data is stored in the process of supplying telephone services or logged in the process of supplying internet services. A detailed definition of individual categories of retained data can be found in Article 54a of the Ordinance on Electronic Communications Networks and Services (Verordnung über elektronische Kommunikationsnetze und –dienste, VKND).<br><br>The ability to store and rapidly transmit retained data to law enforcement authorities is governed by the Communications Act (Articles 52 and 52a et seq.) and the Ordinance on Electronic Communications Networks and Services (Articles 54a and 60-61).<br><br>With regard to which service providers are required to participate in surveillance under the Communications Act and thus also to store retained data, the following should be taken into account:<br><br>According to Article 3(1)(8) of the Communications Act, an electronic communications service is a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting. It does not include information society services, as defined in the legislation on electronic commerce, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks. This entails that from the perspective of communications law, it must be examined for each service of a service provider whether the service consists wholly or mainly in the conveyance of signals on electronic communications networks, in order to assess whether the service or service provider concerned is covered by the scope of application of communications law or not. Only if the service consists wholly or mainly in the conveyance of signals on electronic communications networks is the service provider subject to communications law with regard to that service, and thus also obligated to participate in surveillance in accordance with communications law as well as to store retained data. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | The procedure for ordering surrender of computer data is governed by §§ 96 et seq. StPO. In all cases, a court ruling is required for seizure (in contrast to preservation of evidence).<br><br>1b. The scope of the forwarded data is governed by the same provisions of laws and ordinances discussed above in relation to Article 17(1a). The scope of the data is defined in such a way that both the service provider and the path through which the communication was transmitted can be determined.<br><br>Article 17(1)(b) of the Convention sets out that the service provider compelled to preserve retained data must disclose to the State party's competent authorities a sufficient amount of the traffic data to identify further service providers and path through which the communication was transmitted. The requesting authorities must specify the desired data in sufficient detail. Articles 52 and 52a et seq. of the Communications Act in conjunction with Articles 54a and 60-61 VKND and the procedure for ordering surrender set out in §§ 96 et seq. StPO implement this article in Liechtenstein. |
| **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 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; | 1a. The obligation to surrender all computer data set out in Article 18(1)(a) of the Cybercrime Convention is governed by the Code of Criminal Procedure. According to § 96(2a) StPO, every person must grant access to information saved on data carriers and on request hand over an electronic data carrier or have such a data carrier produced. A backup copy of the data may also be produced, and the production thereof must be permitted.<br><br>1b. Under Article 53(2) of the Communications Act, service providers are obliged to provide the National Police with information on the recorded subscriber data without delay upon written requests, if the data is absolutely necessary for the fulfilment of their legal duties...<br><br>3. Article 18(3) of the Convention defines the term "subscriber information". Liechtenstein law does not define the terms as set out in the Convention, but the terms "Standortdaten" ("location data") and "Teilnehmerdaten" ("subscriber data") in combination do correspond to the definition in the Convention. According to Article 3(1)(47) of the Communications Act, "location data" means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service. And according to Article 3(1)(48) of the Communications Act, "subscriber data" means all personal data required for the establishment, processing, modification or termination of the contractual relationship between |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement. | the user and the provider or for the production and publication of directories, especially name or business name and mailing address of the subscriber as well as relevant means of identification. |
| **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.<br>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. | Because the preconditions for searches of computer systems should be the same as searches for non-digital evidence, the national rules governing the gathering and preservation of evidence are applied. The legal basis is set out in §§ 92 et seq. of the Code of Criminal Procedure.<br><br>1. According to § 93(1) of the Code of Criminal Procedure, a search takes place after prior questioning of the person to be searched. In some cases, this questioning may be waived. The reasons are when the search is being conducted of especially notorious persons, if there is an imminent danger, or if the search is being conducted in premises open to the public. As a rule, searches require a judicial ruling.<br><br>2. An expansion of the search to include other computer systems is therefore subject to the same provisions described in the remarks on Article 19(1) of the Cybercrime Convention.<br><br>3. Seizure of information on data carriers is governed by § 96(2a) StPO. This article governs the possibility of seizure and permission of the production of a backup copy by the competent authority.<br><br>4. According to § 96(2) StPO, every person is obliged to surrender objects subject to seizure on request or to permit the seizure in another way. If the person refuses, coercive penalties may be imposed. Moreover, providers of publicly available electronic communications services and operators of a public communications network are required under § 52(1) of the Communications Act to provide appropriate technical possibilities to monitor an electronic communication and to participate to the required extent in the surveillance. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | |
| **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. | 1 and 2. According to Article 52(1) of the Communications Act, providers of publicly available electronic communications services and operators of a public communications network are inter alia required to provide appropriate technical possibilities to enable the competent authorities to monitor an electronic communication in accordance with the provisions of the Code of Criminal Procedure (§ 102a and § 103)<br><br>(a) and to participate to the required extent in the surveillance of an electronic communication in accordance with the provisions of the Code of Criminal Procedure<br><br>(b). The ordinance provisions are contained in Articles 60 et seq. VKND.<br><br>3. Article 52b of the Communications Act governs verification of data protection. The Liechtenstein Data Protection Office verifies application of the data protection and data security provisions in regard to data processed for the purpose of participating in surveillance. |
| **Article 21 – Interception of content data**<br>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>ito collect or record through the application of technical means on the territory of that Party, or | 1 and 2. § 103 StPO and Article 52(1)(a) and (b) of the Communications Act in conjunction with Articles 60 et seq. VKND permit the collection of content data in real-time, including the obligation of the provider in question to provide appropriate technical capabilities and to cooperate with the competent authorities, solely for the purpose of participating in the surveillance of an electronic communication in accordance with the provisions of the Code of Criminal Procedure.<br><br>3. See response to Article 20(3) of the Cybercrime Convention. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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. | |
| ***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.<br>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. | The scopes of jurisdiction enumerated in Article 22 of the Cybercrime Convention are governed by the Criminal Code in Liechtenstein. 1a is covered by § 62 (offences in Liechtenstein), 1b and c by § 63 (offences committed on board Liechtenstein ships or aircraft), and 1d and 3 by § 65 (Offences abroad that are punished only if they carry a penalty under the laws of the place where they are committed). |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution. | |
| **Chapter III – International co-operation** | |
| **Article 24 – Extradition**<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.<br>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 | 1. Under Liechtenstein law (Article 11 of the Mutual Legal Assistance Act, Rechtshilfegesetz, RHG), extradition is permissible only if the underlying offence is punishable with imprisonment of more than one year under Liechtenstein law. Dual criminality is a necessary condition for the provision of mutual legal assistance. Liechtenstein has not concluded any further extradition treaties after joining the Cybercrime Convention.<br><br>6. The principle "aut dedere aut judicare" is also applied in Liechtenstein. A State party on whose territory a suspect is located must immediately present a case to the competent authorities for the purpose of prosecution if extradition is refused solely on grounds of the suspect's citizenship or because the State party believes that it has jurisdiction itself. This is guaranteed by § 65(1) StGB.<br><br>7. Upon ratification of the Cybercrime Convention, the following declaration was also transmitted to the Secretary General of the Council of Europe: "Liechtenstein declares that according to Article 24, paragraph 7, of the Convention, the member of Government responsible for the Ministry of Justice decides about sending and receiving requests for extradition or provisional arrest." |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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**<br>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 | 2. If certain investigative measures are requested by way of mutual legal assistance, the Mutual Legal Assistance Act (Article 9(1)) provides that the Liechtenstein Code of Criminal Procedure shall be applied, which forms the legal basis for applying the investigative measures envisaged in the Convention.<br><br>3. Expedited means of communication, including fax or e-mail, are permissible when transmitting requests for mutual legal assistance in urgent circumstances, as long as the original copy of the request or other communication is subsequently transmitted by post.<br><br>4. Also for Liechtenstein, the rule applies that the provision of mutual legal assistance, including the grounds on which cooperation is refused, is in principle governed by the law of the requested State party or subject to the conditions provided for in the applicable mutual legal assistance treaties. Mutual legal assistance may not be refused solely on the ground that the request refers to a fiscal offence.<br><br>5. According to the Mutual Legal Assistance Act (Article 51(1)(1)), the provision of mutual legal assistance is impermissible if the precondition of dual criminality is not met. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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 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. | Spontaneous transmission of information is governed by Article 54a of the Liechtenstein Mutual Legal Assistance Act. According to that provision, the court may spontaneously transmit to a foreign authority information that it has obtained for its own criminal proceedings if an international agreement provides a basis for such transmission, this information might be helpful for the opening or carrying out of investigations or proceedings of a foreign authority, and the transmission of the information would also be permissible within the framework of a request for mutual legal assistance by the foreign authority.<br><br>The transmission of information is permissible even without an international agreement if it must be assumed that the content of the information may help prevent an extraditable offence or avert an immediate and serious threat to public security, and if transmission of the information would also be permissible within the framework of a request for mutual legal assistance by the foreign authority.<br><br>The conditions for such transmission is that the transmitted information may not be used without prior consent of the transmitting authority for any purpose other than the purpose giving rise to the transmission, and that the transmitted data must immediately be deleted or corrected by the receiving authority as soon as it turns out that the data is incorrect, or the transmitting authority communicates that the data has been gathered or transmitted unlawfully, or it turns out that the data is not or no longer needed for the purpose giving rise to the transmission. |
| **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 | 2a. The central authority for receiving and sending requests for mutual legal assistance in Liechtenstein is the Office of Justice. With the reorganisation of the National Administration in 2012, the Office of Justice was entrusted with the |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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.<br>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. | responsibilities of the central authority for international mutual legal assistance in criminal matters.<br><br>2b. The Office of Justice, as the competent central authority in Liechtenstein, communicates almost daily with other central authorities by way of direct communication.<br><br>2c and 2d. Upon ratification of the Cybercrime Convention, the following declaration was also transmitted to the Secretary General of the Council of Europe: "In accordance with Article 27, paragraph 2, of the Convention, the Office of Justice is the authority responsible for sending and receiving legal requests for mutual assistance."<br><br>3. This also constitutes a basic principle set out in national law (Article 58 RHG), which is therefore generally followed in practice.<br><br>5. No explicit analogous provision is found in national law, but where essential national interests take precedence, mutual legal assistance may be refused – or, as a lesser measure, refused for a limited period of time – if granting it were to endanger domestic proceedings (Article 2 RHG), especially if evidence is required for such domestic proceedings (Article 52(2) and (3) RHG). But in practice, this option is hardly ever used.<br><br>6. As mentioned in regard to paragraph 5, this option is hardly ever used. But in general terms, Liechtenstein enters into contact with the requesting authorities if questions or potential problems arise in practice in order to find the best possible solution, especially in regard to the application of procedural coercive measures to obtain the necessary information, because the requesting authority often makes requests based on its own legal system, which often necessitates analogous application. In practice, the goal is to provide mutual legal assistance in as comprehensive and timely a manner as possible (Article 1(1) of the European Convention on Mutual Assistance in Criminal Matters (ECMA)).<br><br>7. These requirements are likewise generally already applied in regard to all requests for mutual legal assistance – even where there is no international agreement – in accordance with Article 19 ECMA. In practice, the receipt of a request for mutual legal assistance is confirmed by transmitting a form containing the necessary contact information (case number, name of the assigned judge, direct phone number, fax, and email). Once the procedure is concluded, the requesting authority is informed without delay; the same is true if problems arise while processing the request. In this context, it should also be noted that direct |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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 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. | contact with the requesting authority is preferred in practice in order to avoid delays (and misunderstandings).<br><br>8. Requests may be kept confidential, but this depends very heavily on the measures requested. For instance, it is de facto not possible to keep the blocking of an account or a house search confidential, even if confidentiality may sometimes be requested in this context. In contrast, register extracts and the like are not a problem. Obtaining banking records is possible while maintaining confidentiality, but the person concerned must be given a fair hearing before the records are handed over to the requesting authority. At that time at the latest, inspection of the files must generally also be granted. Already now, requesting authorities are regularly informed of this in practice. The usual approach is to consult with the requesting authority and then obtain the records while maintaining confidentiality in order to save time, but completion of the procedure and the fair hearing is delayed until confidentiality is lifted. See also the remarks on Article 16(3).<br><br>9. Upon ratification of the Cybercrime Convention, the following declaration was also transmitted to the Secretary General of the Council of Europe: "Liechtenstein declares that in case of emergency, within the context of Article 27, paragraph 9, of the Convention, the Office of Justice is the central authority to which all requests to Liechtenstein for mutual assistance must be addressed." |
| **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: | For lack of other applicable provisions, the Liechtenstein authorities apply the national Mutual Legal Assistance Act (RHG) to requests by States with which no treaty arrangement exists. In such cases, the Cybercrime Convention constitutes a superior legal norm, and the RHG applies only on a subsidiary and complementary basis.<br><br>Pursuant to national law, the Liechtenstein authorities apply the rule of speciality as a general matter and not only in regard to requests by States with which no treaty arrangement exists. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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;<br>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 | 1. Requests for the preservation and transmission of data occur regularly in practice, but they are hardly based on the Cybercrime Convention. It should be noted in this regard that mutual legal assistance in regard to electronic data – whether the preservation of existing data or the collection of data through interception – can generally be granted on the basis of the RHG even without an international treaty basis. In Europe, requests are usually based on the ECMA, however.<br><br>2. The requirements are regularly met, but where they are not, a correction must be requested. These requirements essentially also correspond to Article 14 ECMA, so that a certain practice has established itself in Europe.<br><br>3 and 4. Expedited processing is ensured in Liechtenstein, especially if the request is transmitted directly to the Court of Justice, which is always also responsible for ordering the requested measures in its function as the court responsible for mutual legal assistance. Expedited execution in Liechtenstein is aided by the short channels of communication and the simplified structure of public authorities; urgent requests may often be implemented on the same day, provided they are complete and depending on the time they arrive. In mutual legal assistance in criminal matters, Liechtenstein does however reserve the principle of dual criminality and has made a reservation in this regard: "Liechtenstein will... refuse a request for mutual assistance to order the preservation of stored computer data, as provided for under Article 16 of the Convention, if the condition of dual criminality is not fulfilled; this does not apply to the offences established in accordance with Articles 2 through 11 of this Convention." |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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 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. | 5. It cannot be ascertained whether there has been a case of application with reference to the Cybercrime Convention to date, given that other legal bases – especially the ECMA – are generally applied.<br><br>6. If problems are expected relating to completion of a request for mutual legal assistance, the requesting authority is in general informed thereof, irrespective of the legal basis. This happens regularly in practice; see also Article 27(8). |
| **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. | As a general rule, obtained data may be handed over to the requesting authority only upon conclusion of the procedure. If domestic criminal proceedings in which the same information is available are being conducted at the same time, data obtained in those proceedings may be transmitted spontaneously to a foreign authority under Article 54a RHG, however. In such cases, attention must be paid that mutual legal assistance is not circumvented. But transmission of the name of a further provider in a third country does not appear to be problematic in this regard. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | |
| **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. | The requirements can be readily complied with in practice. See the remarks on Article 29(3) and (4) in this regard. The necessary means for compulsory preservation of evidence are available domestically and have proven themselves in practice. |
| **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:<br>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. | This form of mutual legal assistance is to be granted if domestic law provides for such surveillance of traffic data in similar cases. According to the Liechtenstein Code of Criminal Procedure (§ 103), surveillance of electronic communication is only permissible, however, if wilful commission of an offence punishable with more than one year of imprisonment is to be expected. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| **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. | § 103 StPO can be applied in such cases, also in regard to text messages (see response to Article 33). |
| **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;<br>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. | The authority to be established in accordance with Article 35 of the Cybercrime Convention must have the capacity to carry out communications with the points of contact of other States parties on an expedited basis. Coordination with the authorities responsible for mutual legal assistance on an expedited basis is also required.<br><br>The Liechtenstein National Police has been dealing with the question of internet surveillance since 2001, and it maintains a specialized unit for the investigation of computer and internet offences. This unit joined the G8 24/7 network of contact points to combat cybercrime in summer 2008. The unit thus meets the requirements of the 24/7 point of contact as set out in Article 35. |
| **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, | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
| --- | --- |
| 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