Japan

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Version 01 May 2020

Table of contents

[reference to the provisions of the Budapest Convention]

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

www.coe.int/cybercrime

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

State:	
Signature of the Budapest Convention:	23/11/2001
Ratification/accession:	03/07/2012

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data": For the purposes of this Convention: a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; c "service provider" means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service; d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service	
Chapter II – Measures to be taken at the national level	
Section 1 – Substantive criminal law	
Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems	
Article 2 – Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when	**Act on Prohibition of Unauthorized Computer Access** **Article 2**

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.	The term "Act of Unauthorized Computer Access" as used in this Act means any of the following acts: (i) An act of rendering a Specified Computer with an Access Control Feature available for Specified Use that is subject to restrictions imposed by the Access Control Feature concerned by inputting someone else's identification code associated with the Access Control Feature concerned via a telecommunications line and thus operating the Specified Computer concerned (excluding such an act engaged in by the Access Administrator who has added the Access Control Feature concerned and such an act engaged in upon obtaining permission from the Access Administrator concerned or the Authorized User to whom the identification code concerned belongs) (ii) An act of rendering a Specified Computer with an Access Control Feature available for Specified Use that is subject to restrictions imposed by the Access Control Feature concerned by inputting any information (excluding an identification code) or command suitable for evading the restrictions on said Specified Use via a telecommunications line and thus operating the Specified Computer concerned (excluding such an act engaged in by the Access Administrator who has added the Access Control Feature concerned and such an act engaged in upon obtaining permission from the Access Administrator concerned; the same applies in the following item) (iii) An act of rendering a Specified Computer available for Specified Use that is subject to restrictions imposed by the Access Control Feature of another Specified Computer connected thereto via a telecommunications line by inputting any information or command suitable for evading said restrictions into said other Specified Computer via a telecommunications line and thus operating the Specified Computer concerned **Article 3** It is prohibited for any person to engage in an Act of Unauthorized Computer Access. **Article 11** Any person who has violated the provisions of Article 3 shall be punished by imprisonment with work for not more than three years or a fine of not more than 1 million yen.
Article 3 – Illegal interception	**Telecommunications Business Act**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the 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.	**Article 4** (1) The secrecy of communications handled by a telecommunications carrier must not be violated. **Article 179** (1) A person that has violated the secrecy of communications handled by a telecommunications carrier (including communications set forth in Article 164, paragraph (3)) is punished by not more than two years or a fine of not more than one million yen. (2) A person engaging in telecommunications business that has undertaken the act set forth in the preceding paragraph is punished by imprisonment of not more than three years or a fine of not more than two million yen. **Radio Act** **Article 109-2** (1) When any person, who has intercepted encrypted communications or mediates encrypted communications and has received the relevant encrypted communications, has decoded their content for the purposes of divulging or taking advantage of secrets contained in the relevant encrypted communications, that person is guilty of an offense and liable to imprisonment for a period not exceeding one year or to a fine not exceeding five hundred thousand yen. (2) Any person engaged in a radio communications service who commits a crime under the preceding paragraph (limited to cases of interception or reception of encrypted communications related to the service) is guilty of an offense and liable to imprisonment for a period not exceeding two years or to a fine not exceeding one million yen. (3) The term "encrypted communications" in the preceding two paragraphs means radio communications that are processed to prevent the content from being decoded by persons other than parties to the communication (including a person that mediates the relevant communications and is authorized to decode its content). **Wire Telecommunications Act** (this law is not translated) **Article 9, 14**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 4 – Data interference 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	**Penal Code** **Article 161-2** (1) A person who, with the intent to bring about improper administration of the matters of another person, unlawfully creates without due authorization an electronic or magnetic record which is for use in such improper administration and is related to rights, duties or certification of facts, shall be punished by imprisonment for not more than 5 years or a fine of not more than 500,000 yen. (2) When the crime prescribed under the preceding paragraph is committed in relation to an electronic or magnetic record to be created by a public office or a public officer, the offender shall be punished by imprisonment for not more than 10 years or a fine of not more than 1,000,000 yen shall be imposed. **Article 168-2** (1) A person who, without legitimate grounds, creates or provides any of the following records including electronic or magnetic records for the purpose of using them for executing commands on another person's computer is punished by imprisonment for not more than 3 years or a fine of not more than 500,000 yen: (i) Electronic or magnetic records that give unauthorized commands to prevent a computer from performing functions in line with the user's intention or have it perform functions against the user's intention; (ii) Beyond what is set forth in the preceding item, records including electronic or magnetic records in which unauthorized commands referred to in the same item are described. (2) The same applies to a person who, without legitimate grounds, uses electronic or magnetic records set forth in item (i) of the preceding paragraph for the execution of commands on another person's computer. **Article 234-2** (1) A person who obstructs the business of another by interfering with the operation of a computer utilized for the business of the other or by causing such computer to operate counter to the purpose of such utilization by damaging such computer or any electronic or magnetic record used by such computer, by inputting false data or giving unauthorized commands or by any other means, shall be punished by imprisonment for not more than 5 years or a fine of not more than 1,000,000 yen.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Article 258 A person who damages a document or an electronic or magnetic record in use by a public office shall be punished by imprisonment for not less than 3 months but not more than 7 years. **Article 259** A person who damages a document or electronic or magnetic record of another that concerns rights or duties shall be punished by imprisonment for not more than 5 years.
Article 5 – System interference Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data	**Penal Code** **Article 234-2** (1) A person who obstructs the business of another by interfering with the operation of a computer utilized for the business of the other or by causing such computer to operate counter to the purpose of such utilization by damaging such computer or any electronic or magnetic record used by such computer, by inputting false data or giving unauthorized commands or by any other means, shall be punished by imprisonment for not more than 5 years or a fine of not more than 1,000,000 yen. **Article 261** A person who damages or injures property not prescribed under the preceding three Articles shall be punished by imprisonment for not more than 3 years, a fine of not more than 300,000 yen or a petty fine.
Article 6 – Misuse of devices 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of: i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,	**Penal Code** **Article 168-2** (1) A person who, without legitimate grounds, creates or provides any of the following records including electronic or magnetic records for the purpose of using them for executing commands on another person's computer is punished by imprisonment for not more than 3 years or a fine of not more than 500,000 yen: (i) Electronic or magnetic records that give unauthorized commands to prevent a computer from performing functions in line with the user's intention or have it perform functions against the user's intention;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.	(ii) Beyond what is set forth in the preceding item, records including electronic or magnetic records in which unauthorized commands referred to in the same item are described. (2) The same applies to a person who, without legitimate grounds, uses electronic or magnetic records set forth in item (i) of the preceding paragraph for the execution of commands on another person's computer. **Article 168-3** A person who, without legitimate grounds, acquires or stores records including electronic or magnetic records set forth in the items of paragraph (1) of the preceding Article for the purpose referred to in the same paragraph is punished by imprisonment for not more than 2 years or a fine of not more than 300,000 yen. **Act on Prohibition of Unauthorized Computer Access** **Article 4** It is prohibited for any person to obtain someone else's identification code associated with an Access Control Feature for the purpose of engaging in an Act of Unauthorized Computer Access (limited to the kind specified in Article 2, paragraph (4), item (i); the same applies in Article 6 and Article 12, item (ii)). **Article 5** It is prohibited for any person, unless there are justifiable grounds for refusing to do so or any other legitimate reason therefor, to supply someone else's identification code associated with an Access Control Feature to a person other than the Access Administrator associated with the Access Control Feature concerned and the Authorized User to whom the identification code concerned belongs. **Article 6** It is prohibited for any person to store someone else's identification code associated with an Access Control Feature that has been wrongfully obtained for the purpose of engaging in an Act of Unauthorized Computer Access.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Article 12 Any person who falls under any of the following items shall be punished by imprisonment with work for not more than one year or a fine of not more than 500,000 yen. (i) A person :person who has violated the provisions of Article 4 (ii) A person who has supplied the identification code of another person in violation of the provisions of Article 5 despite knowing that the recipient intends to use it for an Act of Unauthorized Computer Access (iii) A person who has violated the provisions of Article 6 **Article 13** Any person who has violated the provisions of Article 5 (excluding a person specified in item (ii) of the preceding article) shall be punished by a fine of not more than 300,000 yen.
Title 2 – Computer-related offences	
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	**Penal Code** **Article 161-2** (1) A person who, with the intent to bring about improper administration of the matters of another person, unlawfully creates without due authorization an electronic or magnetic record which is for use in such improper administration and is related to rights, duties or certification of facts, shall be punished by imprisonment for not more than 5 years or a fine of not more than 500,000 yen. (2) When the crime prescribed under the preceding paragraph is committed in relation to an electronic or magnetic record to be created by a public office or a public officer, the offender shall be punished by imprisonment for not more than 10 years or a fine of not more than 1,000,000 yen shall be imposed.
Article 8 – Computer-related fraud Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system,	**Penal Code** **Article 235** A person who steals the property of another commits the crime of theft and shall be punished by imprisonment for not more than 10 years or a fine of not more than 500,000 yen. **Article 246** (1) A person who defrauds another of property shall be punished by imprisonment for not more than 10 years. (2) The same shall apply to a person who obtains or causes another to obtain a profit by the means prescribed under the preceding paragraph.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.	**Article 246-2** In addition to the provisions of Article 246, a person who obtains or causes another to obtain a profit by creating a false electronic or magnetic record relating to acquisition, loss or alteration of property rights by inputting false data or giving unauthorized commands to a computer utilized for the business of another, or by putting a false electronic or magnetic record relating to acquisition, loss or alteration of property rights into use for the administration of the matters of another shall be punished by imprisonment for not more than 10 years.
Title 3 – Content-related offences	
Article 9 – Offences related to child pornography 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct	**Act on Regulation and Punishment of Acts Relating to Child Prostitution and Child Pornography, and the Protection of Children** **Article 2** (1) The term "Child" as used in this Act means a person under 18 years of age. (3) The term "Child Pornography" as used in this Act means photographs, recording medium containing electronic or magnetic records (meaning a record used in computerized information processing which is created in electronic form, magnetic form, or any other form that cannot be perceived by the human senses; the same applies hereinafter) or any of the following medium which depicts the image of a Child, in a form recognizable by the sense of sight: (i) any image of sexual intercourse or any conduct similar to sexual intercourse with a Child or between Children; (ii) any image of a Child having the Genital Organs, etc. touched by another person or of a Child touching another person's Genital Organs, etc. which arouses or stimulates sexual desire; or (iii) any image of a Child wholly or partially naked, in which sexual body parts of the Child (genital organs or the parts around them, buttocks or chest) are exhibited or emphasized and arouses or stimulates sexual desire. **Article 7** (1) Any person who possesses Child Pornography for the purpose of satisfying one's sexual curiosity (limited to those who have come to possess it voluntarily, and are clearly deemed to as such.) is punished by imprisonment for not more than 1 year or a fine of not more than 1, 000, 000 yen. The same applies to any person who retains electronic or magnetic records falling under any of the items of paragraph 3 of Article 2 depicting the image of a Child in a form recognizable by the sense of sight for the purpose of satisfying one's sexual

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. 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.	curiosity (limited to those who have come to retain it voluntarily, and are clearly deemed to as such.). (2) Any person who provides Child Pornography is punished by imprisonment for not more than 3 years or a fine of not more than 3, 000, 000 yen. The same applies to any person who provides through telecommunication lines electronic or magnetic records falling under any of the items of paragraph 3 of Article 2 depicting the image of a Child in a form recognizable by the sense of sight or other records. (3) Any person who produces, possesses, transports, imports to or exports from Japan Child Pornography for the purpose of the acts prescribed in the preceding paragraph is punished by the same penalty prescribed in the paragraph. The same applies to any person who retains the electronic or magnetic records prescribed in the preceding paragraph for the purpose of the same acts. (4) Beyond the preceding paragraph, any person who produces Child Pornography by having a Child pose in a way falling under any of the items of paragraph 3 of Article 2, and depicting such pose in photographs, recording medium containing electronic or magnetic records or any other medium is punished by the same penalty prescribed in paragraph 2 of this article. (5) Beyond the preceding two paragraphs, any person who produces Child Pornography by secretly depicting the pose of a Child falling under any of the items of paragraph 3 of Article 2, in photographs, recording medium containing electronic or magnetic records or any other is punished by the same penalty prescribed in paragraph 2 of this article. (6) Any person who provides Child Pornography to many or unspecified persons, or displays it in public is punished by imprisonment for not more than 5 years, a fine of not more than 5, 000, 000 yen or both. The same applies to any person who, through telecommunication lines, provides electronic or magnetic records falling under any of the items of paragraph 3 of Article 2 depicting the image of a Child in a form recognizable by the sense of sight or other records to many or unspecified persons. (7) Any person who produces, possesses, transports, imports to or exports from Japan Child Pornography for the purpose of the acts prescribed in the preceding paragraph is punished by the same penalty prescribed in the same paragraph. The same applies to any person who retains the electronic or magnetic records prescribed in the preceding paragraph for the purpose of the same acts. (8) Any Japanese national who imports or exports Child Pornography to or from a foreign country for the purpose of the acts prescribed in paragraph 6 of this article is punished by the same penalty prescribed in the same paragraph.
Title 4 – Offences related to infringements of copyright and related rights	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 10 – Offences related to infringements of copyright and related rights 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	**Copyright Act** **Article 119** (1) A person that infringes a copyright, print rights, or neighboring rights (other than one that personally reproduces a work or performance, etc. for the purpose of private use as referred to in Article 30, paragraph (1) (including as applied mutatis mutandis pursuant to Article 102, paragraph (1); same applies in paragraph (3)); one whose action is deemed to constitute infringement of a copyright, print rights, or neighboring rights pursuant to the provisions of Article 113, paragraph (3); one whose action is deemed to constitute infringement of a copyright or neighboring rights (including rights deemed to be neighboring rights pursuant to the provisions of Article 113, paragraph (5); the same applies in Article 120-2, item (iii)) pursuant to the provisions of Article 113, paragraph (4); one whose action is deemed to constitute infringement of a copyright or neighboring rights pursuant to the provisions of Article 113, paragraph (6); or a person set forth in item (iii) or (iv) of the following paragraph) is subject to imprisonment for a term of up to ten years, a fine of up to ten million yen, or both. (2) A person falling under any of the following items is subject to imprisonment for a term of up to five years, a fine of up to five million yen, or both: (i) a person that infringes the moral rights of an author or the moral rights of a performer (other than one whose action is deemed to constitute infringement of an author's moral rights or a performer's moral rights pursuant to the provisions of Article 113, paragraph (4)); (ii) a person that, for commercial purposes, causes an automated duplicator referred to in Article 30, paragraph (1), item (i) to be used to reproduce a work or performance, etc. as constitutes an infringement of a copyright, print rights, or neighboring rights; (iii) a person that engages in an action that is deemed to constitute infringement of a copyright, print rights, or neighboring rights pursuant to the provisions of Article 113, paragraph (1); (iv) a person that engages in an action that is deemed to constitute infringement of a copyright pursuant to the provisions of Article 113, paragraph (2). (3) A person that infringes a copyright or neighboring rights by digitally recording, for the purpose of private use as referred to in Article 30, paragraph (1), the sound or visuals of a fee-based recorded work, etc. (meaning a work or performance, etc. (limited to one that is the subject of a copyright or neighboring

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	rights) that has undergone sound or visual recording and that is being made available or presented to the public for value (limited to those that are made available or presented to the public without infringing any copyrights or neighboring rights)) that has been transmitted to the public via an automatic public transmission that infringes a copyright or neighboring rights (including an automatic public transmission that is transmitted abroad and that would constitute a copyright or neighboring rights infringement if it were transmitted in Japan), knowing that the automatic public transmission constitutes an infringement, is subject to imprisonment for a term of up to two years, a fine of up to two million yen, or both.
Article 11 – Attempt and aiding or abetting 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention. 3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	**Penal Code** **Article 61** (1) A person who induces another to commit a crime shall be dealt with in sentencing as a principal. (2) The same shall apply to a person who induces another to induce. **Article 62** (1) A person who aids a principal is an accessory. (2) A person who induces an accessory shall be dealt with in sentencing as an accessory. **Article 168-2** (3) An attempt of the crime referred to in the preceding paragraph is punished. **Article 234-2** (2) An attempt of the crime prescribed under the preceding paragraph is punished. **Article 243** An attempt of the crimes prescribed under Articles 235 through 236, and 238 through 240, and paragraph (3) of Article 241 is punished. **Article 250** An attempt of the crimes prescribed under this Chapter shall be punished. **Telecommunications Business Act** **Article 179** (3) An attempt to commit the offenses set forth in the preceding two paragraphs is subject to punishment. **Radio Act**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Article 109-2(4) Any attempted offense under paragraphs (1) and (2) is punished. **Wire Telecommunications Act** (this law is not translated) **Article 14**
Article 12 – Corporate liability 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a a power of representation of the legal person; b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority. 3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	**Telecommunications Business Act** **Article 190** If any representative of a corporation, or an agent, employee or other worker of a corporation or individual, has committed a violation of provisions set forth in the following items in connection with the business of the corporation or individual, in addition to the offender being subject punishment, the corporation is subject to the fine prescribed respectively in those items and the individual is subject to the fine referred to in the relevant Article: (i) Article 181: fine of not more than one hundred million yen; (ii) Article 177 through Article 188 (except Article 180, Article 181, Article 183 and Article 184): fine set forth in the relevant Article. **Act on Regulation and Punishment of Acts Relating to Child Prostitution and Child Pornography, and the Protection of Children** **Article 11** When a representative of a juridical person or a proxy, employee or any other staff member of a juridical person or of an individual has committed any of the crimes prescribed in Articles 5, 6, or paragraph 2 through 8 of Article 7 with regard to the business of the juridical person or individual, not only the offender is punished but also the juridical person or individual are punished by the fine prescribed in the respective articles. **Copyright Act** **Article 124** (1) If the representative of a corporation (including the administrator of an association or foundation without legal personality) or the agent, employee, or other worker of a corporation or person violates the provisions set forth in one of the following items in connection with the business of that corporation or person, in addition to the offender being subject to punishment, the corporation is subject to punishment by the fine prescribed in the relevant item and the person is subject to punishment by the fine prescribed in the provisions referred to in the relevant item: (i) Article 119, paragraph (1); Article 119, paragraph (2), item (iii) or (iv); or Article 122-2, paragraph (1): a fine of up to three hundred million yen;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(ii) Article 119, paragraph (2), item (i) or (ii) or Article 120 through Article 122: the fine referred to in the relevant of these provisions. **Act on General Incorporated Associations and General Incorporated Foundations** **Article 78** A general incorporated association shall be liable to provide compensation for damages caused to a third party by its representative director or other representatives in the course of performing their duties. **Civil Code** **Article 709** A person that has intentionally or negligently infringed the rights or legally protected interests of another person is liable to compensate for damage resulting in consequence. **Article 715** (1) A person that employs another person for a business undertaking is liable to compensate for damage inflicted on a third party by that person's employees with respect to the execution of that business; provided, however, that this does not apply if the employer exercised reasonable care in appointing the employee or in supervising the business, or if the damage could not have been avoided even if the employer had exercised reasonable care. (2) A person that supervises a business on behalf of the employer also has the liability referred to in the preceding paragraph (3) The provisions of the preceding two paragraphs do not preclude the employer or supervisor from exercising their right to reimbursement against the employee. **Wire Telecommunications Act** (this law is not translated) **Article 18**
Article 13 – Sanctions and measures 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty. 2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are	

Back to the Table of Contents

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. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.	**Code of Criminal Procedure** **Article 197**(3) When a public prosecutor, a public prosecutor's assistant officer or a judicial police officer finds it necessary to execute a seizure or seize records created under a record copying order, said person may specify the necessary electronic or magnetic records out of the electronic or magnetic records pertaining to the transmission source, the transmission destination, the date and time of the transmission and other transmission history of electronic communications which are recorded in the course of business, may determine a time period not exceeding 30 days, and may request in writing a person engaged in the business of providing facilities for conducting electronic communications for use in the communications of other persons or a person establishing facilities for conducting electronic communications capable of acting as an intermediary for the transmissions of many, unspecified persons for the purpose of said person's own business not to erase said history. In this case, if it is deemed no longer necessary to execute the seizure or seize records created under a record copying order with regard to said electronic or magnetic records, said person must revoke such request.

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.	(5) When a request pursuant to the provisions of paragraph (2) or paragraph (3) is to be made, if it is necessary, a request may be made that the particulars relating to such request not be divulged without reason. **Article 218** (1) Public prosecutors, public prosecutor's assistant officers or judicial police officials may, when it is necessary for the investigation of an offense, conduct a search, seizure, seizure of records created under a record copying order, or inspection upon a warrant issued by a judge. In this case, the inspection and examination of a person must be conducted upon a warrant for physical examination. (2) Where the article to be seized is a computer, and with regard to a recording medium connected via telecommunication lines to such computer, it may be reasonably supposed that such recording medium was used to retain electronic or magnetic records, which have been made or altered using such computer or electronic or magnetic records which may be altered or erased using such computer, the computer or other recording medium may be seized after such electronic or magnetic records have been copied onto such computer or other recording medium. (3) When a suspect is placed under physical restraint, said suspect's fingerprints or a print of their feet may be taken, said suspect's height or weight may be measured and photographs of said suspect may be taken without the warrant set forth in the paragraph (1), only when said suspect is not stripped naked. (4) The warrant set forth in paragraph (1) is issued upon the request of a public prosecutor, a public prosecutor's assistant officer or a judicial police officer. (5) When a public prosecutor, a public prosecutor's assistant officer or a judicial police officer requests a warrant for an inspection and examination of a person, said public prosecutor, public prosecutor's assistant officer or judicial police officer must indicate the reason for the necessity of the inspection and examination, the sex and physical condition of the person to be inspected and examined and other particulars as provided in the Rules of Court. (6) A judge may provide conditions that said judge deems appropriate for the inspection and examination of a person.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 17 – Expedited preservation and partial disclosure of traffic data 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Code of Criminal Procedure** **Article 197**(3) When a public prosecutor, a public prosecutor's assistant officer or a judicial police officer finds it necessary to execute a seizure or seize records created under a record copying order, said person may specify the necessary electronic or magnetic records out of the electronic or magnetic records pertaining to the transmission source, the transmission destination, the date and time of the transmission and other transmission history of electronic communications which are recorded in the course of business, may determine a time period not exceeding 30 days, and may request in writing a person engaged in the business of providing facilities for conducting electronic communications for use in the communications of other persons or a person establishing facilities for conducting electronic communications capable of acting as an intermediary for the transmissions of many, unspecified persons for the purpose of said person's own business not to erase said history. In this case, if it is deemed no longer necessary to execute the seizure or seize records created under a record copying order with regard to said electronic or magnetic records, said person must revoke such request. **Article 218** (1) Public prosecutors, public prosecutor's assistant officers or judicial police officials may, when it is necessary for the investigation of an offense, conduct a search, seizure, seizure of records created under a record copying order, or inspection upon a warrant issued by a judge. In this case, the inspection and examination of a person must be conducted upon a warrant for physical examination. (2) Where the article to be seized is a computer, and with regard to a recording medium connected via telecommunication lines to such computer, it may be reasonably supposed that such recording medium was used to retain electronic or magnetic records, which have been made or altered using such computer or electronic or magnetic records which may be altered or erased using such computer, the computer or other recording medium may be seized after such electronic or magnetic records have been copied onto such computer or other recording medium. (3) When a suspect is placed under physical restraint, said suspect's fingerprints or a print of their feet may be taken, said suspect's height or weight may be measured and photographs of said suspect may be taken without the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	warrant set forth in the paragraph (1), only when said suspect is not stripped naked. (4) The warrant set forth in paragraph (1) is issued upon the request of a public prosecutor, a public prosecutor's assistant officer or a judicial police officer. (5) When a public prosecutor, a public prosecutor's assistant officer or a judicial police officer requests a warrant for an inspection and examination of a person, said public prosecutor, public prosecutor's assistant officer or judicial police officer must indicate the reason for the necessity of the inspection and examination, the sex and physical condition of the person to be inspected and examined and other particulars as provided in the Rules of Court. (6) A judge may provide conditions that said judge deems appropriate for the inspection and examination of a person.
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;	**Code of Criminal Procedure** **Article 99-2** The court may, when it is necessary, seize records created under a record copying order (meaning having a custodian of electronic or magnetic records or a person with the authority to access electronic or magnetic records copy the necessary electronic or magnetic records onto a recording medium or print said records out, and seize said recording medium; the same applies hereinafter). **Article 106** Searches, seizures or seizures of records created under a record copying order outside of the court must be executed on the issuance of a search warrant, seizure warrant or warrant ordering the seizure of records created under a record copying order. **Article 110-2** If the article to be seized is a recording medium containing electronic or magnetic records, the person executing the seizure warrant may execute the measures prescribed in the following items in lieu of said seizure. The same applies to a seizure in court: (i) the person may copy the electronic or magnetic records recorded on the recording medium which is to be seized onto some other recording medium, print them out or transfer them, and may then seize said other recording medium; (ii) the person may have the person subject to the seizure copy the electronic or magnetic records recorded on the recording medium which is to be seized onto

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.	some other recording medium, print them out or transfer them, and may then seize said other recording medium. **Article 197**(2) Public offices or public or private organizations may be asked to make a report on necessary particulars relating to the investigation. **Article 218** (1) Public prosecutors, public prosecutor's assistant officers or judicial police officials may, when it is necessary for the investigation of an offense, conduct a search, seizure, seizure of records created under a record copying order, or inspection upon a warrant issued by a judge. In this case, the inspection and examination of a person must be conducted upon a warrant for physical examination. (2) Where the article to be seized is a computer, and with regard to a recording medium connected via telecommunication lines to such computer, it may be reasonably supposed that such recording medium was used to retain electronic or magnetic records, which have been made or altered using such computer or electronic or magnetic records which may be altered or erased using such computer, the computer or other recording medium may be seized after such electronic or magnetic records have been copied onto such computer or other recording medium. (3) When a suspect is placed under physical restraint, said suspect's fingerprints or a print of their feet may be taken, said suspect's height or weight may be measured and photographs of said suspect may be taken without the warrant set forth in the paragraph (1), only when said suspect is not stripped naked. (4) The warrant set forth in paragraph (1) is issued upon the request of a public prosecutor, a public prosecutor's assistant officer or a judicial police officer. (5) When a public prosecutor, a public prosecutor's assistant officer or a judicial police officer requests a warrant for an inspection and examination of a person, said public prosecutor, public prosecutor's assistant officer or judicial police officer must indicate the reason for the necessity of the inspection and examination, the sex and physical condition of the person to be inspected and examined and other particulars as provided in the Rules of Court.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(6) A judge may provide conditions that said judge deems appropriate for the inspection and examination of a person. **Article 222** (1) The provisions of Article 99, paragraph (1), Article 100, Articles 102 through 105, Articles 110 through 112, Article 114, Article 115 and Articles 118 through 124 apply mutatis mutandis to a search and seizure conducted by a public prosecutor, public prosecutor's assistant officer or a judicial police official pursuant to the provisions of Article 218, Article 220 and the preceding Article, and the provisions of Article 110, Article 111-2, Article 112, Article 114, Article 118, Article 129, Article 131 and Articles 137 through 140 apply mutatis mutandis to the inspection conducted by a public prosecutor, public prosecutor's assistant officer or a judicial police official pursuant to the provisions of Article 218 or Article 220; provided however, that the dispositions prescribed in Articles 122 through 124 may not be executed by a judicial constable. (2) Where searching the suspect pursuant to the provisions of Article 220 requires urgency, the provisions of Article 114, paragraph (2) does not require compliance. (3) The provisions of Article 116 and Article 117 apply mutatis mutandis to searches, seizures or seizures of records created under a record copying order conducted by a public prosecutor, public prosecutor's assistant officer or a judicial police official pursuant to the provisions of Article 218. (4) Public prosecutors, public prosecutor's assistant officers or judicial police officials may not enter, before sunrise or after sunset, the residence of a person, or premises, buildings or vessel guarded by a person for the purpose of inspection pursuant to the provisions of Article 218, unless the warrant contains a written statement that inspection during the night is permitted; provided however, that this does not apply to the places prescribed in Article 117. (5) When an inspection starts before sunset, it may continue even after sunset. (6) Public prosecutors, public prosecutor's assistant officers or judicial police officials may, when it is necessary to conduct a search, seizure or inspection pursuant to the provisions of Article 218, have the suspect attend it. (7) When any person who refuses an inspection and examination of a person is to be imposed a non-criminal fine or to be ordered to compensate for expenses in accordance with the provisions of paragraph (1), the request for such dispositions must be made to the court.
Article 19 – Search and seizure of stored computer data	**Code of Criminal Procedure**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Article 99** (1) The court may, when it is necessary, seize articles of evidence or articles which it is considered should be confiscated; provided however, that this does not apply when so provided otherwise. (2) If the article to be seized is a computer, and with regard to a recording medium connected via telecommunication lines to such computer, it may be reasonably supposed that such recording medium was used to retain electronic or magnetic records which have been made or altered using such computer, or electronic or magnetic records which can be altered or erased using such computer, the computer or other recording medium may be seized after such electronic or magnetic records have been copied onto such computer or other recording medium. (3) The court may specify the articles to be seized and order the owner, possessor or custodian to submit them. **Article 99-2** The court may, when it is necessary, seize records created under a record copying order (meaning having a custodian of electronic or magnetic records or a person with the authority to access electronic or magnetic records copy the necessary electronic or magnetic records onto a recording medium or print said records out, and seize said recording medium; the same applies hereinafter). **Article 102** (1) The court may, when it is necessary, search the body, articles, residence or any other place of the accused. (2) The body, articles, residence or any other place of a person other than the accused may be searched only when it can be reasonably supposed that articles which should be seized exist. **Article 106** Searches, seizures or seizures of records created under a record copying order outside of the court must be executed on the issuance of a search warrant, seizure warrant or warrant ordering the seizure of records created under a record copying order. **Article 110-2** If the article to be seized is a recording medium containing electronic or magnetic records, the person executing the seizure warrant may execute the measures prescribed in the following items in lieu of said seizure. The same applies to a seizure in court:

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(i) the person may copy the electronic or magnetic records recorded on the recording medium which is to be seized onto some other recording medium, print them out or transfer them, and may then seize said other recording medium; (ii) the person may have the person subject to the seizure copy the electronic or magnetic records recorded on the recording medium which is to be seized onto some other recording medium, print them out or transfer them, and may then seize said other recording medium. **Article 111-2** Where the article to be seized is a recording medium containing electronic or magnetic records, the person executing the search warrant or the seizure warrant may ask the person subject to the measure to operate the computer, or for some other form of cooperation. The same applies to a search or seizure in court. **Article 218** (1) Public prosecutors, public prosecutor's assistant officers or judicial police officials may, when it is necessary for the investigation of an offense, conduct a search, seizure, seizure of records created under a record copying order, or inspection upon a warrant issued by a judge. In this case, the inspection and examination of a person must be conducted upon a warrant for physical examination. (2) Where the article to be seized is a computer, and with regard to a recording medium connected via telecommunication lines to such computer, it may be reasonably supposed that such recording medium was used to retain electronic or magnetic records, which have been made or altered using such computer or electronic or magnetic records which may be altered or erased using such computer, the computer or other recording medium may be seized after such electronic or magnetic records have been copied onto such computer or other recording medium. (3) When a suspect is placed under physical restraint, said suspect's fingerprints or a print of their feet may be taken, said suspect's height or weight may be measured and photographs of said suspect may be taken without the warrant set forth in the paragraph (1), only when said suspect is not stripped naked.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(4) The warrant set forth in paragraph (1) is issued upon the request of a public prosecutor, a public prosecutor's assistant officer or a judicial police officer. (5) When a public prosecutor, a public prosecutor's assistant officer or a judicial police officer requests a warrant for an inspection and examination of a person, said public prosecutor, public prosecutor's assistant officer or judicial police officer must indicate the reason for the necessity of the inspection and examination, the sex and physical condition of the person to be inspected and examined and other particulars as provided in the Rules of Court. (6) A judge may provide conditions that said judge deems appropriate for the inspection and examination of a person. **Article 222** (1) The provisions of Article 99, paragraph (1), Article 100, Articles 102 through 105, Articles 110 through 112, Article 114, Article 115 and Articles 118 through 124 apply mutatis mutandis to a search and seizure conducted by a public prosecutor, public prosecutor's assistant officer or a judicial police official pursuant to the provisions of Article 218, Article 220 and the preceding Article, and the provisions of Article 110, Article 111-2, Article 112, Article 114, Article 118, Article 129, Article 131 and Articles 137 through 140 apply mutatis mutandis to the inspection conducted by a public prosecutor, public prosecutor's assistant officer or a judicial police official pursuant to the provisions of Article 218 or Article 220; provided however, that the dispositions prescribed in Articles 122 through 124 may not be executed by a judicial constable. (2) Where searching the suspect pursuant to the provisions of Article 220 requires urgency, the provisions of Article 114, paragraph (2) does not require compliance. (3) The provisions of Article 116 and Article 117 apply mutatis mutandis to searches, seizures or seizures of records created under a record copying order conducted by a public prosecutor, public prosecutor's assistant officer or a judicial police official pursuant to the provisions of Article 218. (4) Public prosecutors, public prosecutor's assistant officers or judicial police officials may not enter, before sunrise or after sunset, the residence of a person, or premises, buildings or vessel guarded by a person for the purpose of inspection pursuant to the provisions of Article 218, unless the warrant contains a written statement that inspection during the night is permitted; provided however, that this does not apply to the places prescribed in Article 117. (5) When an inspection starts before sunset, it may continue even after sunset.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(6) Public prosecutors, public prosecutor's assistant officers or judicial police officials may, when it is necessary to conduct a search, seizure or inspection pursuant to the provisions of Article 218, have the suspect attend it. (7) When any person who refuses an inspection and examination of a person is to be imposed a non-criminal fine or to be ordered to compensate for expenses in accordance with the provisions of paragraph (1), the request for such dispositions must be made to the court.
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Code of Criminal Procedure** **Article 128** The court may, when it is necessary for fact-finding, conduct an inspection. **Article 111-2** Where the article to be seized is a recording medium containing electronic or magnetic records, the person executing the search warrant or the seizure warrant may ask the person subject to the measure to operate the computer, or for some other form of cooperation. The same applies to a search or seizure in court. **Article 142** Articles 111-2 to 114, 118 and 125 apply mutatis mutandis to the inspection. **Article 218** (1) Public prosecutors, public prosecutor's assistant officers or judicial police officials may, when it is necessary for the investigation of an offense, conduct a search, seizure, seizure of records created under a record copying order, or inspection upon a warrant issued by a judge. In this case, the inspection and examination of a person must be conducted upon a warrant for physical examination. (2) Where the article to be seized is a computer, and with regard to a recording medium connected via telecommunication lines to such computer, it may be reasonably supposed that such recording medium was used to retain electronic or magnetic records, which have been made or altered using such computer or electronic or magnetic records which may be altered or erased using such computer, the computer or other recording medium may be seized after such electronic or magnetic records have been copied onto such computer or other recording medium.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(3) When a suspect is placed under physical restraint, said suspect's fingerprints or a print of their feet may be taken, said suspect's height or weight may be measured and photographs of said suspect may be taken without the warrant set forth in the paragraph (1), only when said suspect is not stripped naked. (4) The warrant set forth in paragraph (1) is issued upon the request of a public prosecutor, a public prosecutor's assistant officer or a judicial police officer. (5) When a public prosecutor, a public prosecutor's assistant officer or a judicial police officer requests a warrant for an inspection and examination of a person, said public prosecutor, public prosecutor's assistant officer or judicial police officer must indicate the reason for the necessity of the inspection and examination, the sex and physical condition of the person to be inspected and examined and other particulars as provided in the Rules of Court. (6) A judge may provide conditions that said judge deems appropriate for the inspection and examination of a person. **Article 222** (1) The provisions of Article 99, paragraph (1), Article 100, Articles 102 through 105, Articles 110 through 112, Article 114, Article 115 and Articles 118 through 124 apply mutatis mutandis to a search and seizure conducted by a public prosecutor, public prosecutor's assistant officer or a judicial police official pursuant to the provisions of Article 218, Article 220 and the preceding Article, and the provisions of Article 110, Article 111-2, Article 112, Article 114, Article 118, Article 129, Article 131 and Articles 137 through 140 apply mutatis mutandis to the inspection conducted by a public prosecutor, public prosecutor's assistant officer or a judicial police official pursuant to the provisions of Article 218 or Article 220; provided however, that the dispositions prescribed in Articles 122 through 124 may not be executed by a judicial constable. (2) Where searching the suspect pursuant to the provisions of Article 220 requires urgency, the provisions of Article 114, paragraph (2) does not require compliance. (3) The provisions of Article 116 and Article 117 apply mutatis mutandis to searches, seizures or seizures of records created under a record copying order conducted by a public prosecutor, public prosecutor's assistant officer or a judicial police official pursuant to the provisions of Article 218.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(4) Public prosecutors, public prosecutor's assistant officers or judicial police officials may not enter, before sunrise or after sunset, the residence of a person, or premises, buildings or vessel guarded by a person for the purpose of inspection pursuant to the provisions of Article 218, unless the warrant contains a written statement that inspection during the night is permitted; provided however, that this does not apply to the places prescribed in Article 117. (5) When an inspection starts before sunset, it may continue even after sunset. (6) Public prosecutors, public prosecutor's assistant officers or judicial police officials may, when it is necessary to conduct a search, seizure or inspection pursuant to the provisions of Article 218, have the suspect attend it. (7) When any person who refuses an inspection and examination of a person is to be imposed a non-criminal fine or to be ordered to compensate for expenses in accordance with the provisions of paragraph (1), the request for such dispositions must be made to the court. **Penal Code** **Article 62** (1) A person who aids a principal is an accessory. (2) A person who induces an accessory shall be dealt with in sentencing as an accessory. **Article 103** A person who harbors or enables the escape of another person who has either committed a crime punishable with a fine or heavier punishment or has escaped from confinement is punished by imprisonment for not more than 3 years or a fine of not more than 300,000 yen. **Article 104** A person who spoils, damages, counterfeits or alters evidence relating to a criminal case of another person, or who uses counterfeit or altered evidence, is punished by imprisonment for not more than 3 years or a fine of not more than 300,000 yen.
Article 21 – Interception of content data 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:	**Act on Wiretapping for Criminal Investigation** (this law is not translated) **Article 3, 11, 28**

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Penal Code** **Article 62** (1) A person who aids a principal is an accessory. (2) A person who induces an accessory shall be dealt with in sentencing as an accessory. **Article 103** A person who harbors or enables the escape of another person who has either committed a crime punishable with a fine or heavier punishment or has escaped from confinement is punished by imprisonment for not more than 3 years or a fine of not more than 300,000 yen. **Article 104** A person who spoils, damages, counterfeits or alters evidence relating to a criminal case of another person, or who uses counterfeit or altered evidence, is punished by imprisonment for not more than 3 years or a fine of not more than 300,000 yen.
Section 3 – Jurisdiction	
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this	**Penal Code** **Article 1 (1)** This Code shall apply to anyone who commits a crime within the territory of Japan. (2) The same shall apply to anyone who commits a crime on board a Japanese vessel or aircraft outside the territory of Japan. **Article 2** This Code shall apply to anyone who commits one of the following crimes outside the territory of Japan: (v) The crimes prescribed under Article 154 (Counterfeiting of Imperial or State Documents), 155 (Counterfeiting of Official Documents), 157 (False Entries in the Original of Notarized Deeds) and 158 (Uttering of Counterfeit Official Documents), and the crime concerning an electronic or magnetic record which should be created by a public office or a public official in Article 161-2 (Unauthorized Creation of Electronic or Magnetic Records);

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	**Article 3** This Code shall apply to any Japanese national who commits one of the following crimes outside the territory of Japan: (iii) The crimes prescribed under Articles 159 through 161 (Counterfeiting of Private Documents; Falsifying of Medical Certificates; Utterance of Counterfeit Private Documents) and the crime regarding electronic or magnetic records in Article 161-2 except that which shall fall within item (v) of the preceding Article; (xiii) The crime prescribed under Article 230 (Defamation); (xiv) The crimes prescribed under Articles 235 through 236 (Larceny; Taking Unlawful Possession of Real Estate; Robbery), Articles 238 through 240 (Constructive Robbery; Robbery through Causing Unconsciousness; Robbery Causing Death or Injury), paragraphs (1) and (3) of Article 241 (Robbery or Forcible Sexual Intercourse; Causing Death Thereby), and Article 243 (Attempts); **Article 4-2** In addition to the provisions of Article 2 through the preceding Article, this Code shall also apply to anyone who commits outside the territory of Japan those crimes prescribed under Part II which are governed by a treaty even if committed outside the territory of Japan. **Act on Regulation and Punishment of Acts Relating to Child Prostitution and Child Pornography, and the Protection of Children** **Article 10** The crimes prescribed in Articles 4 through 6, paragraphs 1 through 7 of Article 7, and paragraphs 1 and 3 (limited to the part related to paragraph 1 of the same article) of Article 8 are governed by Article 3 of the Penal Code (Law No. 45 of 1907). **Act on Prohibition of Unauthorized Computer Access** **Article 14** The offenses specified in Article 11 and Article 12, items (i) to (iii), are governed by the provisions of Article 4-2, of the Penal Code (Act No.45 of 1907). **Radio Act** **Article 109-2** (5) (this paragraph is not transrated)

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Act for Enforcement of the Penal Code (this law is not transrated) **Article 27** **Wire Telecommunications Act** (this law is not translated) **Article 14** **Act of Extradition** **Article 2** A fugitive shall not be extradited in any of the following circumstances; provided that this shall not apply in cases falling under items (iii), (iv), (viii), or (ix) when the extradition treaty provides otherwise. (ix) When the fugitive is a Japanese national.
Chapter III – International co-operation	
Article 24 – Extradition 1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply. 2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them. 3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis	**Act of Extradition** (the whole law is relevant)

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
for extradition with respect to any criminal offence referred to in paragraph 1 of this article. 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party. 7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure	
Article 25 – General principles relating to mutual assistance 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.	**Act on International Assistance in Investigation and Other Related Matters** (the whole law is relevant)

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.	
Article 26 – Spontaneous information 1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter. 2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times. 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party. 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities. 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider	**Act on International Assistance in Investigation and Other Related Matters** (the whole law is relevant) **National Public Service Act** **Article 100** (1) An official must not divulge any secret which may have come to the official's knowledge in the course of duties. This also applies after the official has left the position. (2) In order for an official to make a statement concerning any secret in the course of duties as a witness, an expert witness or in other capacities provided for by laws and regulations, the official is to require the permission of the head of the government agency appointing the official (in the case of a person who has retired, the head of the government agency having jurisdiction over the government position the official held at the time of the retirement or any government position equivalent thereto). (3) The permission set forth in the preceding paragraph may not be refused, except in cases pertaining to the conditions and procedures provided for by law or by Cabinet Orders. (4) The provisions of the preceding three paragraphs do not apply where information is requested by the National Personnel Authority during an investigation or hearing conducted by the National Personnel Authority. It is not necessary for any person to secure permission from anyone to make a statement or testify on any confidential or restricted information when so requested by the National Personnel Authority during or as part of such investigations or hearings conducted under the jurisdiction of the National Personnel Authority. Failure to make a statement or testify before the National Personnel Authority on such information upon its request must make the individual liable to the penal provisions of this Act. (5) The provisions of the preceding paragraph apply mutatis mutandis to the investigation conducted by the Reemployment Surveillance Commission, to which the authority is delegated pursuant to the provisions of Article 18-4. In

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
whether the request may be granted partially or subject to such conditions as it deems necessary. 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly. 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party. b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol). c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so. d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party. e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.	this case, the term "National Personnel Authority" in said paragraph is deemed to be replaced with "Reemployment Surveillance Commission," and the term "investigation or hearing" with "investigation."
Article 28 – Confidentiality and limitation on use 1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the	**National Public Service Act**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or b not used for investigations or proceedings other than those stated in the request. 3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it. 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.	**Article 100** (1) An official must not divulge any secret which may have come to the official's knowledge in the course of duties. This also applies after the official has left the position. (2) In order for an official to make a statement concerning any secret in the course of duties as a witness, an expert witness or in other capacities provided for by laws and regulations, the official is to require the permission of the head of the government agency appointing the official (in the case of a person who has retired, the head of the government agency having jurisdiction over the government position the official held at the time of the retirement or any government position equivalent thereto). (3) The permission set forth in the preceding paragraph may not be refused, except in cases pertaining to the conditions and procedures provided for by law or by Cabinet Orders. (4) The provisions of the preceding three paragraphs do not apply where information is requested by the National Personnel Authority during an investigation or hearing conducted by the National Personnel Authority. It is not necessary for any person to secure permission from anyone to make a statement or testify on any confidential or restricted information when so requested by the National Personnel Authority during or as part of such investigations or hearings conducted under the jurisdiction of the National Personnel Authority. Failure to make a statement or testify before the National Personnel Authority on such information upon its request must make the individual liable to the penal provisions of this Act. (5) The provisions of the preceding paragraph apply mutatis mutandis to the investigation conducted by the Reemployment Surveillance Commission, to which the authority is delegated pursuant to the provisions of Article 18-4. In this case, the term "National Personnel Authority" in said paragraph is deemed to be replaced with "Reemployment Surveillance Commission," and the term "investigation or hearing" with "investigation."
Article 29 – Expedited preservation of stored computer data 1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data. 2 A request for preservation made under paragraph 1 shall specify:	**Act on International Assistance in Investigation and Other Related Matters** **Article 2** Assistance shall not be provided in any of the following circumstances:

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
a the authority seeking the preservation; b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; c the stored computer data to be preserved and its relationship to the offence; d any available information identifying the custodian of the stored computer data or the location of the computer system; e the necessity of the preservation; and f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data. 3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation. 4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. 5 In addition, a request for preservation may only be refused if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 4 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the	(i) When the offense for which assistance is requested is a political offense, or when the request for assistance is deemed to have been made with a view to investigating a political offense; (ii) Unless otherwise provided by a treaty, when the act constituting the offense for which assistance is requested would not constitute a crime under laws and regulations of Japan were it to be committed in Japan; (iii) With respect to a request for examination of a witness or provision of articles of evidence, unless otherwise provided by a treaty, when the requesting country does not clearly demonstrate in writing that the evidence is essential to the investigation. **Article 8** (1) With regard to the collection of evidence necessary for assistance, a public prosecutor or a judicial police officer may take the following measures; (vi) To request in writing, the person engaged in the business of providing facilities operating electronic communications for the use of the communications of other persons or the person establishing facilities operating electronic communications capable of intermediating the transmissions of many, unspecified persons for the purpose of its own business, to not erase transmission history of specified necessary electromagnetic records out of the electromagnetic records pertaining to the transmission source, the transmission destination, the date and time of the transmission and other transmission history of the electronic communications which are recorded in the course of business, for a period not exceeding 30 days (in case of an extension, a period not exceeding a total of 60 days). (2) With regard to the collection of evidence necessary for assistance, a public prosecutor or a judicial police officer may, if it is deemed to be necessary, undertake seizure, seizure ordering records, search, or inspection of evidence, upon a warrant issued by a judge.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.	
Article 30 – Expedited disclosure of preserved traffic data 1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted. 2 Disclosure of traffic data under paragraph 1 may only be withheld if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	**Act on International Assistance in Investigation and Other Related Matters** **Article 8** (1) With regard to the collection of evidence necessary for assistance, a public prosecutor or a judicial police officer may take the following measures; (vi) To request in writing, the person engaged in the business of providing facilities operating electronic communications for the use of the communications of other persons or the person establishing facilities operating electronic communications capable of intermediating the transmissions of many, unspecified persons for the purpose of its own business, to not erase transmission history of specified necessary electromagnetic records out of the electromagnetic records pertaining to the transmission source, the transmission destination, the date and time of the transmission and other transmission history of the electronic communications which are recorded in the course of business, for a period not exceeding 30 days (in case of an extension, a period not exceeding a total of 60 days). (2) With regard to the collection of evidence necessary for assistance, a public prosecutor or a judicial police officer may, if it is deemed to be necessary, undertake seizure, seizure ordering records, search, or inspection of evidence, upon a warrant issued by a judge.
Article 31 – Mutual assistance regarding accessing of stored computer data 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where: a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or	**Act on International Assistance in Investigation and Other Related Matters** **Article 8** (2) With regard to the collection of evidence necessary for assistance, a public prosecutor or a judicial police officer may, if it is deemed to be necessary, undertake seizure, seizure ordering records, search, or inspection of evidence, upon a warrant issued by a judge.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	
Article 33 – Mutual assistance in the real-time collection of traffic data 1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	**Act on International Assistance in Investigation and Other Related Matters** **Article 8** (2) With regard to the collection of evidence necessary for assistance, a public prosecutor or a judicial police officer may, if it is deemed to be necessary, undertake seizure, seizure ordering records, search, or inspection of evidence, upon a warrant issued by a judge.
Article 34 – Mutual assistance regarding the interception of content data The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.	
Article 35 – 24/7 Network 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects. 2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis. 3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.	
Article 42 – Reservations By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.	

Back to the Table of Contents