UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
UN Convention Chapter I – General provisions	
Article 2. Use of terms For the purposes of this Convention: (a) "Information and communications technology system" shall mean any device or group of interconnected or related devices, one or more of which, pursuant to a program, gathers, stores and performs automatic processing of electronic data; (b) "Electronic data" shall mean any representation of facts, information or concepts in a form suitable for processing in an information and communications technology system, including a program suitable to cause an information and communications technology system to perform a function; (c) "Traffic data" shall mean any electronic data relating to a communication by means of an information and communications technology system, generated by an information and communications technology 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; (d) "Content data" shall mean any electronic data, other than subscriber information or traffic data, relating to the substance of the data transferred by an information and communications technology system, including, but not limited to, images, text messages, voice messages, audio recordings and video recordings; (e) "Service provider" shall mean any public or private entity that: (i) Provides to users of its service the ability to communicate by means of an information and communications technology system; or	**BC Article 1 – Definitions** 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. **BC Article 9 – Offenses 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:

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
(ii) Processes or stores electronic data on behalf of such a communications service or users of such a service; (f) "Subscriber information" shall mean any information 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: (i) The type of communications service used, the technical provisions related thereto and the period of service; (ii) The subscriber's identity, postal or geographical address, telephone or other access number, billing or payment information, available on the basis of the service agreement or arrangement; (iii) Any other information on the site of the installation of communications equipment, available on the basis of the service agreement or arrangement; (g) "Personal data" shall mean any information relating to an identified or identifiable natural person; "Serious crime" shall mean conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty; (h) "Serious crime" shall mean conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty; (i) "Property" shall mean assets of every kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, including virtual assets, and legal documents or instruments evidencing title to, or interest in, such assets; (j) "Proceeds of crime" shall mean any property derived from or obtained, directly or indirectly, through the commission of an offence; (k) "Freezing" or "seizure" shall mean temporarily prohibiting the transfer,	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. 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. **BC Article 18 – Subscriber Information** 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

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
conversion, disposition or movement of property or temporarily assuming custody or control of property on the basis of an order issued by a court or other competent authority; (l) "Confiscation", which includes forfeiture where applicable, shall mean the permanent deprivation of property by order of a court or other competent authority; (m) "Predicate offence" shall mean any offence as a result of which proceeds have been generated that may become the subject of an offence as defined in article 17 of this Convention; (n) "Regional economic integration organization" shall mean an organization constituted by sovereign States of a given region to which its member States have transferred competence in respect of matters governed by this Convention and which has been duly authorized, in accordance with its internal procedures, to sign, ratify, accept, approve or accede to it; references to "States Parties" under this Convention shall apply to such organizations within the limits of their competence; (o) "Emergency" shall mean a situation in which there is a significant and imminent risk to the life or safety of any natural person.	and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement. **Second Protocol Article 3 – Definitions** a "central authority" means the authority or authorities designated under a mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the Parties concerned, or, in the absence thereof, the authority or authorities designated by a Party under Article 27, paragraph 2.a, of the Convention; b "competent authority" means a judicial, administrative or other law-enforcement authority that is empowered by domestic law to order, authorise or undertake the execution of measures under this Protocol for the purpose of collection or production of evidence with respect to specific criminal investigations or proceedings; c "emergency" means a situation in which there is a significant and imminent risk to the life or safety of any natural person; d "personal data" means information relating to an identified or identifiable natural person; e "transferring Party" means the Party transmitting the data in response to a request or as part of a joint investigation team or, for the purposes of Chapter II, section 2, a Party in whose territory a transmitting service provider or entity providing domain name registration services is located.
Article 3. Scope of application This Convention shall apply, except as otherwise stated herein, to:	**Second Protocol Article 2 – Scope of Application**

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
(a) The prevention, investigation and prosecution of the criminal offences established in accordance with this Convention, including the freezing, seizure, confiscation and return of the proceeds from such offences; (b) The collecting, obtaining, preserving and sharing of evidence in electronic form for the purpose of criminal investigations or proceedings, as provided for in articles 23 and 35 of this Convention. **Article 4. Offenses established in accordance with other United Nations conventions and protocols** 1. In giving effect to other applicable United Nations conventions and protocols to which they are Parties, States Parties shall ensure that criminal offences established in accordance with such conventions and protocols are also considered criminal offences under domestic law when committed through the use of information and communications technology systems. 2. Nothing in this article shall be interpreted as establishing criminal offences in accordance with this Convention.	1 Except as otherwise specified herein, the measures described in this Protocol shall be applied: a as between Parties to the Convention that are Parties to this Protocol, to specific criminal investigations or proceedings concerning criminal offences related to computer systems and data, and to the collection of evidence in electronic form of a criminal offence; and b as between Parties to the First Protocol that are Parties to this Protocol, to specific criminal investigations or proceedings concerning criminal offences established pursuant to the First Protocol. 2 Each Party shall adopt such legislative and other measures as may be necessary to carry out the obligations set forth in this Protocol.
Article 5. Protection of sovereignty 1. States Parties shall carry out their obligations under this Convention in a manner consistent with the principles of sovereign equality and territorial integrity of States and that of non-intervention in the domestic affairs of other States. 2. Nothing in this Convention shall entitle a State Party to undertake in the territory of another State the exercise of jurisdiction and performance of functions that are reserved exclusively for the authorities of that other State by its domestic law.	
Article 6. Respect for human rights	

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
1. States Parties shall ensure that the implementation of their obligations under this Convention is consistent with their obligations under international human rights law. 2. Nothing in this Convention shall be interpreted as permitting suppression of human rights or fundamental freedoms, including the rights related to the freedoms of expression, conscience, opinion, religion or belief, peaceful assembly and association, in accordance and in a manner consistent with applicable international human rights law.	
UN Convention Chapter II – Criminalization	
Article 7. Illegal access 1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as a criminal offence under its domestic law, when committed intentionally, the access to the whole or any part of an information and communications technology system without right. 2. A State Party may require that the offence be committed by infringing security measures, with the intent of obtaining electronic data or other dishonest or criminal intent or in relation to an information and communications technology system that is connected to another information and communications technology system.	**BC Article 2 – Illegal access** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.
Article 8. Illegal interception 1. Each State 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 interception, made by technical means, of non-public transmissions of electronic data to, from or within an information and communications technology system, including electromagnetic emissions from an information and communications technology system carrying such electronic data.	**BC Article 3 – Illegal Interception** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
2. A State Party may require that the offence be committed with dishonest or criminal intent, or in relation to an information and communications technology system that is connected to another information and communications technology system. **Chapter VI Preventative measures — Article 53(3)(e). Preventative measures** 3. Preventive measures may include: (e) Recognizing the contributions of the legitimate activities of security researchers when intended solely, and to the extent permitted and subject to the conditions prescribed by domestic law, to strengthen and improve the security of service providers' products, services and customers located within the territory of the State Party;	committed with dishonest intent, or in relation to a computer system that is connected to another computer system.
Article 9. Interference with electronic data 1. Each State 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 damaging, deletion, deterioration, alteration or suppression of electronic data. 2. A State Party may require that the conduct described in paragraph 1 of this article result in serious harm.	**BC 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.
Article 10. Interference with an information and communications technology system Each State 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 serious hindering of the functioning of an information and communications technology system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing electronic data.	**BC 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.

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
Article 11. Misuse of devices 1. Each State 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 obtaining, production, sale, procurement for use, import, distribution or otherwise making available of: (i) A device, including a program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with articles 7 to 10 of this convention; or (ii) A password, access credentials, electronic signature or similar data by which the whole or any part of an information and communications technology system is capable of being accessed; with the intent that the device, including a program, or the password, access credentials, electronic signature or similar data be used for the purpose of committing any of the offences established in accordance with articles 7 to 10 of this Convention; and (b) The possession of an item referred to in paragraph 1 (a) (i) or (ii) of this article, with intent that it be used for the purpose of committing any of the offences established in accordance with articles 7 to 10 of this Convention. 2. This article shall not be interpreted as imposing criminal liability where the obtaining, production, sale, procurement for use, import, distribution or otherwise making available, or the possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with articles 7 to 10 of this Convention, such as for the authorized testing or protection of an information and communications technology system.	**BC Article 6 – Misuse of devices** 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of: i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 Each Party may reserve the right not to apply paragraph 1 of this article, 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.

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
3. Each State 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.	
Article 12 Information and communications technology system-related forgery 1. Each State 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 electronic data resulting in inauthentic data with the intent that they be considered or acted upon for legal purposes as if they were authentic, regardless of whether or not the data are directly readable and intelligible. 2. A State Party may require an intent to defraud, or a similar dishonest or criminal intent, before criminal liability attaches.	**BC 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.
Article 13. Information and communications technology system-related theft or fraud Each State Party shall adopt such legislative and other measures as may be necessary to establish as a criminal offence under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by means of: (a) Any input, alteration, deletion or suppression of electronic data; (b) Any interference with the functioning of an information and communications technology system; (c) Any deception as to factual circumstances made through an information and communications technology system that causes a person to do or omit to do anything which that person would not otherwise do or omit to do;	**BC Article 8 – Computer-related fraud** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
with the fraudulent or dishonest intent of procuring for oneself or for another person, without right, a gain in money or other property.	
Article 14. Offences related to online child sexual abuse or child sexual exploitation material 1. Each State 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, offering, selling, distributing, transmitting, broadcasting, displaying, publishing or otherwise making available child sexual abuse or child sexual exploitation material through an information and communications technology system; (b) Soliciting, procuring or accessing child sexual abuse or child sexual exploitation material through an information and communications technology system; (c) Possessing or controlling child sexual abuse or child sexual exploitation material stored in an information and communications technology system or another storage medium; (d) Financing the offences established in accordance with subparagraphs (a) to (c) of this paragraph, which States Parties may establish as a separate offence. 2. For the purposes of this article, the term "child sexual abuse or child sexual exploitation material" shall include visual material, and may include written or audio content, that depicts, describes or represents any person under 18 years of age: (a) Engaging in real or simulated sexual activity; (b) In the presence of a person engaging in any sexual activity; (c) Whose sexual parts are displayed for primarily sexual purposes; or	**BC Article 9 – Offenses 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. 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.

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
(d) Subjected to torture or cruel, inhumane or degrading treatment or punishment and such material is sexual in nature. 3. A State Party may require that the material identified in paragraph 2 of this article be limited to material that: (a) Depicts, describes or represents an existing person; or (b) Visually depicts child sexual abuse or child sexual exploitation. 4. An accordance with their domestic law and consistent with applicable international obligations, States Parties may take steps to exclude the criminalization of: (a) Conduct by children for self-generated material depicting them; or (b) The consensual production, transmission, or possession of material described in paragraph 2 (a) to (c) of this article, where the underlying conduct depicted is legal as determined by domestic law, and where such material is maintained exclusively for the private and consensual use of the persons involved. 5. Nothing in this Convention shall affect any international obligations which are more conducive to the realization of the rights of the child.	4 Each party may reserve the right not to apply, in whole or in part, paragraphs 1, subparagraphs d and e, and 2, sub-paragraphs b and c.
	BC Article 10 – Offenses 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.

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
	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.
Article 15. Solicitation or grooming for the purpose of committing a sexual offence against a child 1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the act of intentionally communicating, soliciting, grooming, or making any arrangement through an information and communications technology system for the purpose of committing a sexual offence against a child, as defined in domestic law, including for the commission of any of the offences established in accordance with article 14 of this Convention. 2. A State Party may require an act in furtherance of the conduct described in paragraph 1 of this article. 3. A State Party may consider extending criminalization in accordance with paragraph 1 of this article in relation to a person believed to be a	

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
child. 4. States Parties may take steps to exclude the criminalization of conduct as described in paragraph 1 of this article when committed by children.	
Article 16 Non-consensual dissemination of intimate images 1. Each State 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 selling, distributing, transmitting, publishing or otherwise making available of an intimate image of a person by means of an information and communications technology system, without the consent of the person depicted in the image. 2. For the purpose of paragraph 1 of this article, "intimate image" shall mean a visual recording of a person over the age of 18 years made by any means, including a photograph or video recording, that is sexual in nature, in which the person's sexual parts are exposed or the person is engaged in sexual activity, which was private at the time of the recording, and in respect of which the person or persons depicted maintained a reasonable expectation of privacy at the time of the offence. 3. A State Party may extend the definition of intimate images, as appropriate, to depictions of persons who are under the age of 18 years if they are of legal age to engage in sexual activity under domestic law and the image does not depict child abuse or exploitation. 4. For the purposes of this article, a person who is under the age of 18 years and depicted in an intimate image cannot consent to the dissemination of an intimate image that constitutes child sexual abuse or child sexual exploitation material under article 14 of this Convention.	

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
5. A State Party may require the intent to cause harm before criminal liability attaches. 6. States Parties may take other measures concerning matters related to this article, in accordance with their domestic law and consistent with applicable international obligations.	
Article 17. Laundering of proceeds of crime 1. Each State Party shall adopt, in accordance with fundamental principles of its domestic law, such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally: (a) (i) The conversion or transfer of property, knowing that such property is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of that person's actions; (ii) The concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime; (b) Subject to the basic concepts of its legal system: (i) The acquisition, possession or use of property, knowing, at the time of receipt, that such property is the proceeds of crime; (ii) Participation in, association with or conspiracy to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the offences established in accordance with this article. 2. For purposes of implementing or applying paragraph 1 of this article: (a) Each State Party shall establish as predicate offences relevant offences established in accordance with articles 7 to 16 of this	

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
Convention; (b) In the case of States Parties whose legislation sets out a list of specific predicate offences, they shall, at a minimum, include in that list a comprehensive range of offences established in accordance with articles 7 to 16 of this Convention; (c) For the purposes of subparagraph (b) of this paragraph, predicate offences shall include offences committed both within and outside the jurisdiction of the State Party in question. However, offences committed outside the jurisdiction of a State Party shall constitute predicate offences only when the relevant conduct is a criminal offence under the domestic law of the State where it is committed and would be a criminal offence under the domestic law of the State Party implementing or applying this article, had it been committed there; (d) Each State Party shall furnish copies of its laws that give effect to this article and of any subsequent changes to such laws or a description thereof to the Secretary-General of the United Nations; (e) If required by fundamental principles of the domestic law of a State Party, it may be provided that the offences set forth in paragraph 1 of this article do not apply to the persons who committed the predicate offence; (f) Knowledge, intent or purpose required as an element of an offence set forth in paragraph 1 of this article may be inferred from objective factual circumstances.	
Article 18. Liability of legal persons 1. Each State Party shall adopt such measures as may be necessary, consistent with its legal principles, to establish the liability of legal persons for participation in the offences established in	**BC 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

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
accordance with this Convention. 2. Subject to the legal principles of the State Party, the liability of legal persons may be criminal, civil or administrative. 3. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offences. 4. Each State Party shall, in particular, ensure that legal persons held liable in accordance with this article are subject to effective, proportionate and dissuasive criminal or non-criminal sanctions, including monetary sanctions	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.
Article 19. Participation and attempt 1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as a criminal offence, in accordance with its domestic law, when committed intentionally, the participation in any capacity, such as that of an accomplice, assistant or instigator, in an offence established in accordance with this Convention. 2. Each State Party may adopt the necessary legislative and other measures to establish as a criminal offence, in accordance with its domestic law, when committed intentionally, any attempt to commit an offence established in accordance with this Convention. 3. Each State Party may adopt the necessary legislative and other measures	**BC 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.

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
to establish as a criminal offence, in accordance with its domestic law, when committed intentionally, the preparation for an offence established in accordance with this Convention.	3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.
Article 21(4). Prosecution, adjudication and sanctions 4. Each State Party shall ensure that any person prosecuted for offences established in accordance with this Convention enjoys all rights and guarantees in conformity with domestic law and consistent with the applicable international obligations of the State Party, including the right to a fair trial and the rights of the defence.	**BC 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
UN Convention Chapter III – Jurisdiction	
Article 22. Jurisdiction 1. Each State Party shall adopt such measures as may be necessary to establish its jurisdiction over the offences established in accordance with this Convention when: (a) The offence is committed in the territory of that State Party; or (b) The offence is committed on board a vessel that is flying the flag of that State Party or an aircraft that is registered under the laws of that State Party at the time when the offence is committed. 2. Subject to article 5 of this Convention, a State Party may also establish its jurisdiction over any such offence when: (a) The offence is committed against a national of that State Party; or	**BC 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.

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
(b) The offence is committed by a national of that State Party or a stateless person with habitual residence in its territory; or (c)The offence is one of those established in accordance with article 17, paragraph 1 (b) (ii), of this Convention and is committed outside its territory with a view to the commission of an offence established in accordance with article 17, paragraph 1 (a) (i) or (ii) or (b) (i), of this Convention within its territory; or (d) The offence is committed against the State Party. 3. For the purposes of article 37, paragraph 11, of this Convention, each State Party shall take such measures as may be necessary to establish its jurisdiction over the offences established in accordance with this Convention when the alleged offender is present in its territory and it does not extradite such person solely on the ground that the person is one of its nationals. 4. Each State Party may also adopt such measures as may be necessary to establish its jurisdiction over the offences established in accordance with this Convention when the alleged offender is present in its territory and it does not extradite the person. 5. If a State Party exercising its jurisdiction under paragraph 1 or 2 of this article has been notified, or has otherwise learned, that any other States Parties are conducting an investigation, prosecution or judicial proceeding in respect of the same conduct, the competent authorities of those States Parties shall, as appropriate, consult one another with a view to coordinating their actions. 6. Without prejudice to norms of general international law, this Convention shall not exclude the exercise of any criminal jurisdiction established by a State Party in accordance with its domestic law.	2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. 5 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 23. Scope of procedural measures 1. Each State Party shall adopt such legislative and other measures as	**BC Article 14 – Scope of procedural provisions** 1 Each Party shall adopt such legislative and other measures as may be

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
may be necessary to establish the powers and procedures provided for in this chapter for the purpose of specific criminal investigations or proceedings.	necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.
2. Except as provided otherwise in this Convention, each State Party shall apply the powers and procedures referred to in paragraph 1 of this article to: (a) The criminal offences established in accordance with this Convention; (b) Other criminal offences committed by means of an information and communications technology system; and (c) The collection of evidence in electronic form of any criminal offence.	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 State Party may reserve the right to apply the measures referred to in article 29 of this Convention 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 30 of this Convention. Each State Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in article 29; (b) Where a State Party, owing to limitations in its legislation in force at the time of the adoption of this Convention, is not able to apply the measures referred to in articles 29 and 30 of this Convention to communications being transmitted within an information and communications technology system of a service provider which: (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 information and communications technology system, whether public or	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

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
private; that State Party may reserve the right not to apply these measures to such communications. Each State Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in articles 29 and 30 of this Convention.	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.
UN Convention Chapter IV – Procedural measures and law enforcement	
Article 23. Scope of procedural measures	**BC Article 14 – Scope of procedural provisions**
1. Each State Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this chapter for the purpose of specific criminal investigations or proceedings.	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 provided otherwise in this Convention, each State Party shall apply the powers and procedures referred to in paragraph 1 of this article to: (a) The criminal offences established in accordance with this Convention; (b) Other criminal offences committed by means of an information and communications technology system; and (c) The collection of evidence in electronic form of any criminal offence.	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 State Party may reserve the right to apply the measures referred to in article 29 of this Convention 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 30 of this Convention. Each State	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.

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in article 29; (b) Where a State Party, owing to limitations in its legislation in force at the time of the adoption of this Convention, is not able to apply the measures referred to in articles 29 and 30 of this Convention to communications being transmitted within an information and communications technology system of a service provider which: (i) Is being operated for the benefit of a closed group of users; and (ii) (ii) Does not employ public communications networks and is not connected with another information and communications technology system, whether public or private; that State Party may reserve the right not to apply these measures to such communications. Each State Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in articles 29 and 30 of this Convention.	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 24. Conditions and safeguards 1. Each State Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this chapter are subject to conditions and safeguards provided for under its domestic law, which shall provide for the protection of human rights, in accordance with its obligations under international human rights law, and which shall incorporate the principle of proportionality. 2. In accordance with and pursuant to the domestic law of each State Party, such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, include, inter alia, judicial or other independent review, the right to an effective remedy, grounds justifying application, and limitation of the scope and the duration of such power or procedure.	**BC Article 15 – Conditions and safeguards** 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
3. To the extent that it is consistent with the public interest, in particular the proper administration of justice, each State Party shall consider the impact of the powers and procedures in this chapter upon the rights, responsibilities and legitimate interests of third parties. 4. The conditions and safeguards established in accordance with this article shall apply at the domestic level to the powers and procedures set forth in this chapter, both for the purpose of domestic criminal investigations and proceedings and for the purpose of rendering international cooperation by the requested State Party. 5. References to judicial or other independent review in paragraph 2 of this article are references to such review at the domestic level.	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. **Second Protocol Article 13 –Conditions and safeguards** In accordance with Article 15 of the Convention, each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Protocol are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties.
Article 25. Expedited preservation of stored electronic data 1. Each State 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 electronic data, including traffic data, content data and subscriber information, that have been stored by means of an information and communications technology system, in particular where there are grounds to believe that the electronic data are particularly vulnerable to loss or modification.	**BC 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

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
	procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.
Article 26. Expedited preservation and partial disclosure of traffic data Each State Party shall adopt, in respect of traffic data that are to be preserved under the provisions of article 25 of this Convention, 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 a communication; and (b) Ensure the expeditious disclosure to the State Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the State Party to identify the service providers and the path through which the communication or indicated information was transmitted.	**BC 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.
Article 27. Production order Each State 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 electronic data in that person's possession or control that are stored in an information and communications technology system or an electronic data storage medium; and (b) A service provider offering its services in the territory of the State Party to submit subscriber information relating to such services in that service provider's possession or control.	**BC 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 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

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
	to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement. **Second Protocol Article 6 – Procedures enhancing direct co-operation: Request for domain name registration information** 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities, for the purposes of specific criminal investigations or proceedings, to issue a request to an entity providing domain name registration services in the territory of another Party for information in the entity's possession or control, for identifying or contacting the registrant of a domain name. 2 Each Party shall adopt such legislative and other measures as may be necessary to permit an entity in its territory to disclose such information in response to a request under paragraph 1, subject to reasonable conditions provided by domestic law. 3 The request under paragraph 1 shall include:

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
	a the date on which the request was issued and the identity and contact details of the competent authority issuing the request; b the domain name about which information is sought and a detailed list of the information sought, including the particular data elements; c a statement that the request is issued pursuant to this Protocol, that the need for the information arises because of its relevance to a specific criminal investigation or proceeding and that the information will only be used for that specific criminal investigation or proceeding; and d the time frame within which and the manner in which to disclose the information and any other special procedural instructions. 4 If acceptable to the entity, a Party may submit a request under paragraph 1 in electronic form. Appropriate levels of security and authentication may be required. 5 In the event of non-co-operation by an entity described in paragraph 1, a requesting Party may request that the entity give a reason why it is not disclosing the information sought. The requesting Party may seek consultation with the Party in which the entity is located, with a view to determining available measures to obtain the information. 6 Each Party shall, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, or at any other time, communicate to the Secretary General of the Council of Europe the authority designated for the purpose of consultation under paragraph 5. 7 The Secretary General of the Council of Europe shall set up and keep updated a register of authorities designated by the Parties under paragraph 6. Each Party shall ensure that the details that it has provided for the register are correct at all times.

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
	Second Protocol Article 7 – Procedures enhancing direct co-operation: Disclosure of subscriber information 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to issue an order to be submitted directly to a service provider in the territory of another Party, in order to obtain the disclosure of specified, stored subscriber information in that service provider's possession or control, where the subscriber information is needed for the issuing Party's specific criminal investigations or proceedings. 2 a Each Party shall adopt such legislative and other measures as may be necessary for a service provider in its territory to disclose subscriber information in response to an order under paragraph 1. b At the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, a Party may – with respect to orders issued to service providers in its territory – make the following declaration: "The order under Article 7, paragraph 1, must be issued by, or under the supervision of, a prosecutor or other judicial authority, or otherwise be issued under independent supervision". 3 The order under paragraph 1 shall specify: a the issuing authority and date issued; b a statement that the order is issued pursuant to this Protocol; c the name and address of the service provider(s) to be served; d the offence(s) that is/are the subject of the criminal investigation or proceeding; e the authority seeking the specific subscriber information, if not the issuing authority; and

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
	f f a detailed description of the specific subscriber information sought. 4 The order under paragraph 1 shall be accompanied by the following supplemental information: a the domestic legal grounds that empower the authority to issue the order; b a reference to legal provisions and applicable penalties for the offence being investigated or prosecuted; c the contact information of the authority to which the service provider shall return the subscriber information, from which it can request further information, or to which it shall otherwise respond; d the time frame within which and the manner in which to return the subscriber information; e whether preservation of the data has already been sought, including the date of preservation and any applicable reference number; f any special procedural instructions; g if applicable, a statement that simultaneous notification has been made pursuant to paragraph 5; and h any other information that may assist in obtaining disclosure of the subscriber information. 5 a A Party may, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, and at any other time, notify the Secretary General of the Council of Europe that, when an order is issued under paragraph 1 to a service provider in its territory, the Party

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
	requires, in every case or in identified circumstances, simultaneous notification of the order, the supplemental information and a summary of the facts related to the investigation or proceeding. b Whether or not a Party requires notification under paragraph 5.a, it may require the service provider to consult the Party's authorities in identified circumstances prior to disclosure. c The authorities notified under paragraph 5.a or consulted under paragraph 5.b may, without undue delay, instruct the service provider not to disclose the subscriber information if: i disclosure may prejudice criminal investigations or proceedings in that Party; or ii conditions or grounds for refusal would apply under Article 25, paragraph 4, and Article 27, paragraph 4, of the Convention had the subscriber information been sought through mutual assistance. d The authorities notified under paragraph 5.a or consulted under paragraph 5.b: i may request additional information from the authority referred to in paragraph 4.c for the purposes of applying paragraph 5.c and shall not disclose it to the service provider without that authority's consent; and ii shall promptly inform the authority referred to in paragraph 4.c if the service provider has been instructed not to disclose the subscriber information and give the reasons for doing so. e A Party shall designate a single authority to receive notification under paragraph 5.a and perform the actions described in paragraphs 5.b, 5.c and 5.d. The Party shall, at the time when notification to the Secretary General of the Council of Europe

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
	under paragraph 5.a is first given, communicate to the Secretary General the contact information of that authority. f The Secretary General of the Council of Europe shall set up and keep updated a register of the authorities designated by the Parties pursuant to paragraph 5.e and whether and under what circumstances they require notification pursuant to paragraph 5.a. Each Party shall ensure that the details that it provides for the register are correct at all times. 6 If acceptable to the service provider, a Party may submit an order under paragraph 1 and supplemental information under paragraph 4 in electronic form. A Party may provide notification and additional information under paragraph 5 in electronic form. Appropriate levels of security and authentication may be required. 7 If a service provider informs the authority in paragraph 4.c that it will not disclose the subscriber information sought, or if it does not disclose subscriber information in response to the order under paragraph 1 within thirty days of receipt of the order or the timeframe stipulated in paragraph 4.d, whichever time period is longer, the competent authorities of the issuing Party may then seek to enforce the order only via Article 8 or other forms of mutual assistance. Parties may request that a service provider give a reason for refusing to disclose the subscriber information sought by the order. 8 A Party may, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, declare that an issuing Party shall seek disclosure of subscriber information from the service provider before seeking it under Article 8, unless the issuing Party provides a reasonable explanation for not having done so. 9 At the time of signature of this Protocol or when depositing its instrument of ratification, acceptance, or approval, a Party may: a reserve the right not to apply this article; or

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
	b if disclosure of certain types of access numbers under this article would be inconsistent with the fundamental principles of its domestic legal system, reserve the right not to apply this article to such numbers.
Article 28. Search and seizure of stored electronic data 1. Each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: (a) An information and communications technology system, part of it, and electronic data stored therein; and (b) An electronic data storage medium in which the electronic data sought may be stored; in the territory of that State Party. 2. Each State Party shall adopt such legislative and other measures as may be necessary to ensure that, where its authorities search or similarly access a specific information and communications technology system or part of it, pursuant to paragraph 1 (a) of this article, and have grounds to believe that the electronic data sought are stored in another information and communications technology system or part of it in its territory, and such data are lawfully accessible from or available to the initial system, such authorities shall be able to expeditiously conduct the search to obtain access to that other information and communications technology system. 3. Each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure electronic data in its territory accessed in accordance with paragraph 1 or 2 of this article. These measures shall include the power to:	**BC Article 19 – Search and seizure of stored computer data** 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a 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;

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
(a) Seize or similarly secure an information and communications technology system or part of it, or an electronic data storage medium; (b) Make and retain copies of those electronic data in electronic form; (c) Maintain the integrity of the relevant stored electronic data; (d) Render inaccessible or remove those electronic data in the accessed information and communications technology system. 4. Each State 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 information and communications technology system in question, the information and telecommunications network, or their component parts, or measures applied to protect the electronic data therein, to provide, as is reasonable, the necessary information to enable the undertaking of the measures referred to in paragraphs 1 to 3 of this article.	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. **Second Protocol Article 8 – Procedures enhancing international co-operation: Giving effect to orders from another party for expedited production of subscriber information and traffic data** 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to issue an order to be submitted as part of a request to another Party for the purpose of compelling a service provider in the requested Party's territory to produce specified and stored a subscriber information, and b traffic data in that service provider's possession or control which is needed for the Party's specific criminal investigations or proceedings. 2 Each Party shall adopt such legislative and other measures as may be necessary to give effect to an order under paragraph 1 submitted by a requesting Party.

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
	3 In its request, the requesting Party shall submit the order under paragraph 1, the supporting information and any special procedural instructions to the requested Party. a The order shall specify: i the issuing authority and the date the order was issued; ii a statement that the order is submitted pursuant to this Protocol; iii the name and address of the service provider(s) to be served; iv the offence(s) that is/are the subject of the criminal investigation or proceeding; v the authority seeking the information or data, if not the issuing authority; and vi a detailed description of the specific information or data sought. b The supporting information, provided for the purpose of assisting the requested Party to give effect to the order and which shall not be disclosed to the service provider without the consent of the requesting Party, shall specify: i the domestic legal grounds that empower the authority to issue the order; ii the legal provisions and applicable penalties for the offence(s) being investigated or prosecuted; iii the reason why the requesting Party believes that the service provider is in possession or control of the data;

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
	iv a summary of the facts related to the investigation or proceeding; v the relevance of the information or data to the investigation or proceeding; vi contact information of an authority or authorities that may provide further information; vii whether preservation of the information or data has already been sought, including the date of preservation and any applicable reference number; and viii whether the information has or data have already been sought by other means, and, if so, in what manner. c The requesting Party may request that the requested Party carry out special procedural instructions. 4 A Party may declare at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, and at any other time, that additional supporting information is required to give effect to orders under paragraph 1. 5 The requested Party shall accept requests in electronic form. It may require appropriate levels of security and authentication before accepting the request. 6 a The requested Party, from the date of receipt of all the information specified in paragraphs 3 and 4, shall make reasonable efforts to serve the service provider within forty-five days, if not sooner, and shall order a return of requested information or data no later than: i twenty days for subscriber information; and

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
	ii forty-five days for traffic data. b The requested Party shall provide for the transmission of the produced information or data to the requesting Party without undue delay. 7 If the requested Party cannot comply with the instructions under paragraph 3.c in the manner requested, it shall promptly inform the requesting Party, and, if applicable, specify any conditions under which it could comply, following which the requesting Party shall determine whether the request should nevertheless be executed. 8 The requested Party may refuse to execute a request on the grounds established in Article 25, paragraph 4, or Article 27, paragraph 4, of the Convention or may impose conditions it considers necessary to permit execution of the request. The requested Party may postpone execution of requests for reasons established under Article 27, paragraph 5, of the Convention. The requested Party shall notify the requesting Party as soon as practicable of the refusal, conditions, or postponement. The requested Party shall also notify the requesting Party of other circumstances that are likely to delay execution of the request significantly. Article 28, paragraph 2.b, of the Convention shall apply to this article. 9 a If the requesting Party cannot comply with a condition imposed by the requested Party under paragraph 8, it shall promptly inform the requested Party. The requested Party shall then determine if the information or material should nevertheless be provided. b If the requesting Party accepts the condition, it shall be bound by it. The requested Party that supplies information or material subject to such a condition may require the requesting Party to explain in relation to that condition the use made of such information or material.

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
	10 Each Party shall, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, communicate to the Secretary General of the Council of Europe and keep up to date the contact information of the authorities designated: a to submit an order under this article; and b to receive an order under this article. 11 A Party may, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, declare that it requires that requests by other Parties under this article be submitted to it by the central authority of the requesting Party, or by such other authority as mutually determined between the Parties concerned. 12 The Secretary General of the Council of Europe shall set up and keep updated a register of authorities designated by the Parties under paragraph 10. Each Party shall ensure that the details that it has provided for the register are correct at all times. 13 At the time of signature of this Protocol or when depositing its instrument of ratification, acceptance, or approval, a Party may reserve the right not to apply this article to traffic data. **Second Protocol Article 9: Procedures enhancing international cooperation: Expedited disclosure of stored computer data in an emergency** 1 a Each Party shall adopt such legislative and other measures as may be necessary, in an emergency, for its point of contact for the 24/7 Network referenced in Article 35 of the Convention ("point of contact") to transmit a request to and receive a request from a point of contact in another Party seeking immediate assistance in obtaining from a service provider in the territory of that Party the expedited disclosure of specified, stored computer data in that

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
	service provider's possession or control, without a request for mutual assistance. b A Party may, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, declare that it will not execute requests under paragraph 1.a seeking only the disclosure of subscriber information. 2 Each Party shall adopt such legislative and other measures as may be necessary to enable, pursuant to paragraph 1: a its authorities to seek data from a service provider in its territory following a request under paragraph 1; b a service provider in its territory to disclose the requested data to its authorities in response to a request under paragraph 2.a; and c its authorities to provide the requested data to the requesting Party. 3 The request under paragraph 1 shall specify: a the competent authority seeking the data and date on which the request was issued; b a statement that the request is issued pursuant to this Protocol; c the name and address of the service provider(s) in possession or control of the data sought; d the offence(s) that is/are the subject of the criminal investigation or proceeding and a reference to its legal provisions and applicable penalties; e sufficient facts to demonstrate that there is an emergency and how the data sought relate to it;

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
	f a detailed description of the data sought; g any special procedural instructions; and h any other information that may assist in obtaining disclosure of the requested data. 4 The requested Party shall accept a request in electronic form. A Party may also accept a request transmitted orally and may require confirmation in electronic form. It may require appropriate levels of security and authentication before accepting the request. 5 A Party may, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, declare that it requires requesting Parties, following the execution of the request, to submit the request and any supplemental information transmitted in support thereof, in a format and through such channel, which may include mutual assistance, as specified by the requested Party. 6 The requested Party shall inform the requesting Party of its determination on the request under paragraph 1 on a rapidly expedited basis and, if applicable, shall specify any conditions under which it would provide the data and any other forms of co-operation that may be available. 7 a If a requesting Party cannot comply with a condition imposed by the requested Party under paragraph 6, it shall promptly inform the requested Party. The requested Party shall then determine whether the information or material should nevertheless be provided. If the requesting Party accepts the condition, it shall be bound by it. b The requested Party that supplies information or material subject to such a condition may require the requesting Party to explain in

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
	relation to that condition the use made of such information or material
Article 29. Real-time collection of traffic data 1. Each State 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 in the territory of that State Party; and (b) Compel a service provider, within its existing technical capability: (i) To collect or record, through the application of technical means in the territory of that State Party; or (ii) To cooperate 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 an information and communications technology system. 2. Where a State Party, owing to the principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1 (a) of this article, it may instead adopt such 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 in that territory. 3. Each State 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.	**BC 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.

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
Article 30. Interception of content data 1. Each State Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious criminal offences to be determined by domestic law, to empower its competent authorities to: (a) Collect or record, through the application of technical means in the territory of that State Party; and (b) Compel a service provider, within its existing technical capability: (i) To collect or record, through the application of technical means in the territory of that State Party; or (ii) To cooperate 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 an information and communications technology system. 2. Where a State Party, owing to the principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1 (a) of this article, it may instead adopt such 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 in that territory. 3. Each State 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.	**BC Article 21 – Interception of content data** 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system.
Article 31. Freezing, seizure and confiscation of the proceeds of crime 1. Each State Party shall adopt, to the greatest extent possible within its domestic legal system, such measures as may be necessary to enable the confiscation of: (a) Proceeds of crime derived from offences established in accordance	

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
with this Convention or property the value of which corresponds to that of such proceeds; (b) Property, equipment or other instrumentalities used in or destined for use in offences established in accordance with this Convention. 2. Each State Party shall adopt such measures as may be necessary to enable the identification, tracing, freezing or seizure of any item referred to in paragraph 1 of this article for the purpose of eventual confiscation. 3. Each State Party shall adopt, in accordance with its domestic law, such legislative and other measures as may be necessary to regulate the administration by the competent authorities of frozen, seized or confiscated property covered in paragraphs 1 and 2 of this article. 4. If proceeds of crime have been transformed or converted, in part or in full, into other property, such property shall be liable to the measures referred to in this article instead of the proceeds. 5. If proceeds of crime have been intermingled with property acquired from legitimate sources, such property shall, without prejudice to any powers relating to freezing or seizure, be liable to confiscation up to the assessed value of the intermingled proceeds. 6. Income or other benefits derived from proceeds of crime, from property into which proceeds of crime have been transformed or converted or from property with which proceeds of crime have been intermingled, shall also be liable to the measures referred to in this article, in the same manner and to the same extent as proceeds of crime. 7. For the purposes of this article and article 50 of this Convention, each State Party shall empower its courts or other competent authorities to order that bank, financial or commercial records be made available or be seized. A State Party shall not decline to act under the provisions of this paragraph on the ground of bank secrecy. 8. Each State Party may consider the possibility of requiring that an	

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
offender demonstrate the lawful origin of alleged proceeds of crime or other property liable to confiscation, to the extent that such a requirement is consistent with the principles of their domestic law and with the nature of the judicial and other proceedings. 9. The provisions of this article shall not be construed as prejudicing the rights of bona fide third parties. 10. Nothing contained in this article shall affect the principle that the measures to which it refers shall be defined and implemented in accordance with the provisions of the domestic law of a State Party.	
UN Convention Chapter V – International cooperation	
Article 35. General Principles of international cooperation 1. States Parties shall cooperate with each other in accordance with the provisions of this Convention, as well as other applicable international instruments on international cooperation in criminal matters, and domestic laws, for the purpose of: (a) The investigation and prosecution of, and judicial proceedings in relation to, the criminal offences established in accordance with this Convention, including the freezing, seizure, confiscation and return of the proceeds from such offences; (b) The collecting, obtaining, preserving and sharing of evidence in electronic form of criminal offences established in accordance with this Convention; (c) The collecting, obtaining, preserving and sharing of evidence in electronic form of any serious crime, including serious crimes established in accordance with other applicable United Nations conventions and protocols in force at the time of the adoption of this Convention.	**Article 23 – General principles relating to international co-operation** The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international cooperation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes 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.

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
2. For the purpose of the collecting, obtaining, preserving and sharing of evidence in electronic form of offences as provided for in paragraph 1 (b) and (c) of this article, the relevant paragraphs of article 40, and articles 41 to 46 of this Convention shall apply. 3. In matters of international cooperation, whenever dual criminality is considered a requirement, it shall be deemed fulfilled irrespective of whether the laws of the requested State Party place the offence within the same category of offence or denominate the offence by the same terminology as the requesting State Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under the laws of both States Parties.	
Article 36. Protection of personal data 1. (a) A State Party transferring personal data pursuant to this Convention shall do so in accordance with its domestic law and any obligations the transferring Party may have under applicable international law. States Parties shall not be required to transfer personal data in accordance with this Convention if the data cannot be provided in compliance with their applicable laws concerning the protection of personal data; (b) Where the transfer of personal data would not be compliant with paragraph 1 (a) of this article, States Parties may seek to impose appropriate conditions, in accordance with such applicable laws, to achieve compliance in order to respond to a request for personal data; (c) States Parties are encouraged to establish bilateral or multilateral arrangements to facilitate the transfer of personal data. 1 For personal data transferred in accordance with this Convention, States Parties shall ensure that the personal data received are subject to effective and appropriate safeguards in the respective legal frameworks of the States Parties.	**BC Article 28 – Confidentiality and limitation on use** 1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or b not used for investigations or proceedings other than those stated in the request. 3 If the requesting Party cannot comply with a condition referred to in 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.

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
2 In order to transfer personal data obtained in accordance with this Convention to a third country or an international organization, a State Party shall notify the original transferring State Party of its intention and request its authorization. The Stat e Party shall transfer such personal data only with the authorization of the original transferring State Party, which may require that the authorization be provided in written form.	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. **Second Protocol Article 14 – Protection of personal data** 1 Scope a Except as otherwise provided in paragraphs 1.b and c, each Party shall process the personal data that it receives under this Protocol in accordance with paragraphs 2 to 15 of this article. b If, at the time of receipt of personal data under this Protocol, both the transferring Party and the receiving Party are mutually bound by an international agreement establishing a comprehensive framework between those Parties for the protection of personal data, which is applicable to the transfer of personal data for the purpose of the prevention, detection, investigation and prosecution of criminal offences, and which provides that the processing of personal data under that agreement complies with the requirements of the data protection legislation of the Parties concerned, the terms of such agreement shall apply, for the measures falling within the scope of such agreement, to personal data received under this Protocol in lieu of paragraphs 2 to 15, unless otherwise agreed between the Parties concerned. c If the transferring Party and the receiving Party are not mutually bound under an agreement described in paragraph 1.b, they may mutually determine that the transfer of personal data under this Protocol may take place on the basis of other agreements or arrangements between the Parties concerned in lieu of paragraphs 2 to 15. d Each Party shall consider that the processing of personal data pursuant to paragraphs 1.a and 1.b meets the requirements of its personal data protection legal framework for international transfers of personal data, and no further authorisation for transfer

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
	shall be required under that legal framework. A Party may only refuse or prevent data transfers to another Party under this Protocol for reasons of data protection under the conditions set out in paragraph 15 when paragraph 1.a applies; or under the terms of an agreement or arrangement referred to in paragraphs 1.b or c, when one of those paragraphs applies. Nothing in this article shall prevent a Party from applying stronger safeguards to the processing by its own authorities of personal data received under this Protocol. 2 Purpose and use a The Party that has received personal data shall process them for the purposes described in Article 2. It shall not further process the personal data for an incompatible purpose, and it shall not further process the data when this is not permitted under its domestic legal framework. This article shall not prejudice the ability of the transferring Party to impose additional conditions pursuant to this Protocol in a specific case, however, such conditions shall not include generic data protection conditions. b The receiving Party shall ensure under its domestic legal framework that personal data sought and processed are relevant to and not excessive in relation to the purposes of such processing. 3 Quality and integrity Each Party shall take reasonable steps to ensure that personal data are maintained with such accuracy and completeness and are as up to date as is necessary and appropriate for the lawful processing of the personal data, having regard to the purposes for which they are processed. 4 Sensitive data Processing by a Party of personal data revealing racial or ethnic origin, political opinions or religious or other beliefs, or trade union membership; genetic data; biometric data considered sensitive in view of the risks

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
	involved; or personal data concerning health or sexual life; shall only take place under appropriate safeguards to guard against the risk of unwarranted prejudicial impact from the use of such data, in particular against unlawful discrimination. 5 Retention periods Each Party shall retain the personal data only for as long as necessary and appropriate in view of the purposes of processing the data pursuant to paragraph 2. In order to meet this obligation, it shall provide in its domestic legal framework for specific retention periods or periodic review of the need for further retention of the data. 6 Automated decisions Decisions producing a significant adverse effect concerning the relevant interests of the individual to whom the personal data relate may not be based solely on automated processing of personal data, unless authorised under domestic law and with appropriate safeguards that include the possibility to obtain human intervention. 7 Data security and security incidents a Each Party shall ensure that it has in place appropriate technological, physical and organisational measures for the protection of personal data, in particular against loss or accidental or unauthorised access, disclosure, alteration or destruction ("security incident"). b Upon discovery of a security incident in which there is a significant risk of physical or nonphysical harm to individuals or to the other Party, the receiving Party shall promptly assess the likelihood and scale thereof and shall promptly take appropriate action to mitigate such harm. Such action shall include notification to the transferring authority or, for purposes of Chapter II, section 2, the authority or authorities designated pursuant to paragraph 7.c. However, notification may include appropriate restrictions as to

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
	the further transmission of the notification; it may be delayed or omitted when such notification may endanger national security, or delayed when such notification may endanger measures to protect public safety. Such action shall also include notification to the individual concerned, unless the Party has taken appropriate measures so that there is no longer a significant risk. Notification to the individual may be delayed or omitted under the conditions set out in paragraph 12.a.i. The notified Party may request consultation and additional information concerning the incident and the response thereto. c Each Party shall, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, communicate to the Secretary General of the Council of Europe the authority or authorities to be notified under paragraph 7.b for the purposes of Chapter II, section 2; the information provided may subsequently be modified. 8 Maintaining records Each Party shall maintain records or have other appropriate means to demonstrate how an individual's personal data are accessed, used and disclosed in a specific case. 9 Onward sharing within a Party a When an authority of a Party provides personal data received initially under this Protocol to another authority of that Party, that other authority shall process it in accordance with this article, subject to paragraph 9.b. b Notwithstanding paragraph 9.a, a Party that has made a reservation under Article 17 may provide personal data it has received to its constituent States or similar territorial entities provided the Party has in place measures in order that the receiving authorities continue to effectively protect the data by

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
	providing for a level of protection of the data comparable to that afforded by this article. c In case of indications of improper implementation of this paragraph, the transferring Party may request consultation and relevant information about those indications. 10 Onward transfer to another State or international organisation a The receiving Party may transfer the personal data to another State or international organisation only with the prior authorisation of the transferring authority or, for purposes of Chapter II, section 2, the authority or authorities designated pursuant to paragraph 10. b Each Party shall, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, communicate to the Secretary General of the Council of Europe the authority or authorities to provide authorisation for purposes of Chapter II, section 2; the information provided may subsequently be modified. 11 Transparency and notice a Each Party shall provide notice through the publication of general notices, or through personal notice to the individual whose personal data have been collected, with regard to: i the legal basis for and the purpose(s) of processing; ii any retention or review periods pursuant to paragraph 5, as applicable; iii recipients or categories of recipients to whom such data are disclosed; and iv access, rectification and redress available.

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
	b A Party may subject any personal notice requirement to reasonable restrictions under its domestic legal framework pursuant to the conditions set forth in paragraph 12.a.i. c Where the transferring Party's domestic legal framework requires giving personal notice to the individual whose data have been provided to another Party, the transferring Party shall take measures so that the other Party is informed at the time of transfer regarding this requirement and appropriate contact information. The personal notice shall not be given if the other Party has requested that the provision of the data be kept confidential, where the conditions for restrictions as set out in paragraph 12.a.i apply. Once these restrictions no longer apply and the personal notice can be provided, the other Party shall take measures so that the transferring Party is informed. If it has not yet been informed, the transferring Party is entitled to make requests to the receiving Party which will inform the transferring Party whether to maintain the restriction. 12 Access and rectification a Each Party shall ensure that any individual, whose personal data have been received under this Protocol is entitled to seek and obtain, in accordance with processes established in its domestic legal framework and without undue delay: i a written or electronic copy of the documentation kept on that individual containing the individual's personal data and available information indicating the legal basis for and purposes of the processing, retention periods and recipients or categories of recipients of the data ("access"), as well as information regarding available options for redress; provided that access in a particular case may be subject to the application of proportionate restrictions permitted under its domestic legal framework, needed, at the time of adjudication, to protect the rights and

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
	freedoms of others or important objectives of general public interest and that give due regard to the legitimate interests of the individual concerned; ii rectification when the individual's personal data are inaccurate or have been improperly processed; rectification shall include – as appropriate and reasonable considering the grounds for rectification and the particular context of processing – correction, supplementation, erasure or anonymisation, restriction of processing, or blocking. b If access or rectification is denied or restricted, the Party shall provide to the individual, in written form which may be provided electronically, without undue delay, a response informing that individual of the denial or restriction. It shall provide the grounds for such denial or restriction and provide information about available options for redress. Any expense incurred in obtaining access should be limited to what is reasonable and not excessive. 13 Judicial and non-judicial remedies Each Party shall have in place effective judicial and non-judicial remedies to provide redress for violations of this article. 14 Oversight Each Party shall have in place one or more public authorities that exercise, alone or cumulatively, independent and effective oversight functions and powers with respect to the measures set forth in this article. The functions and powers of these authorities acting alone or cumulatively shall include investigation powers, the power to act upon complaints and the ability to take corrective action. 15 Consultation and suspension A Party may suspend the transfer of personal data to another Party if it has substantial evidence that the other Party is in systematic or material breach

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
	of the terms of this article or that a material breach is imminent. It shall not suspend transfers without reasonable notice, and not until after the Parties concerned have engaged in a reasonable period of consultation without reaching a resolution. However, a Party may provisionally suspend transfers in the event of a systematic or material breach that poses a significant and imminent risk to the life or safety of, or substantial reputational or monetary harm to, a natural person, in which case it shall notify and commence consultations with the other Party immediately thereafter. If the consultation has not led to a resolution, the other Party may reciprocally suspend transfers if it has substantial evidence that suspension by the suspending Party was contrary to the terms of this paragraph. The suspending Party shall lift the suspension as soon as the breach justifying the suspension has been remedied; any reciprocal suspension shall be lifted at that time. Any personal data transferred prior to suspension shall continue to be treated in accordance with this Protocol.
Article 37. Extradition 1. This article shall apply to the criminal offences established in accordance with this Convention where the person who is the subject of the request for extradition is present in the territory of the requested State Party, provided that the offence for which extradition is sought is punishable under the domestic law of both the requesting State Party and the requested State Party. When the extradition is sought for the purpose of serving a final sentence of imprisonment or another form of detention imposed in respect of an extraditable offence, the requested State Party may grant the extradition in accordance with domestic law. 2. Notwithstanding paragraph 1 of this article, a State Party whose law so permits may grant the extradition of a person for any of the criminal offences established in accordance with this Convention that are not punishable under its own domestic law.	**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

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
3. If the request for extradition includes several separate criminal offences, at least one of which is extraditable under this article and some of which are not extraditable by reason of their period of imprisonment but are related to offences established in accordance with this Convention, the requested State Party may apply this article also in respect of those offences. 4. Each of the offences to which this article applies shall be deemed to be included as an extraditable offence in any extradition treaty existing between States Parties. States Parties undertake to include such offences as extraditable offences in every extradition treaty to be concluded between them. 5. If a State Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another State Party with which it has no extradition treaty, it may consider this Convention the legal basis for extradition in respect of any offence to which this article applies. 6. States Parties that make extradition conditional on the existence of a treaty shall: (a) At the time of deposit of their instruments of ratification, acceptance or approval of or accession to this Convention, inform the Secretary-General of the United Nations whether they will take this Convention as the legal basis for cooperation in extradition with other States Parties to this Convention; and (b) If they do not take this Convention as the legal basis for cooperation in extradition, seek, where appropriate, to conclude treaties on extradition with other States Parties to this Convention in order to implement this article. 7. States Parties that do not make extradition conditional on the existence of a treaty shall recognize offences to which this article applies as extraditable offences between themselves. 8. Extradition shall be subject to the conditions provided for by the domestic law of the requested State Party or by applicable extradition treaties, including, inter alia, conditions in relation to the minimum	existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them. 3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article. 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party. 7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
penalty requirement for extradition and the grounds upon which the requested State Party may refuse extradition. 9. States Parties shall, subject to their domestic law, endeavour to expedite extradition procedures and to simplify evidentiary requirements relating thereto in respect of any offence to which this article applies. 10. Subject to the provisions of its domestic law and its extradition treaties, the requested State Party may, upon being satisfied that the circumstances so warrant and are urgent, and at the request of the requesting State Party, including when the request is transmitted through existing channels of the International Criminal Police Organization, take a person whose extradition is sought and who is present in its territory into custody or take other appropriate measures to ensure the person's presence at extradition proceedings. 11. A State Party in whose territory an alleged offender is found, if it does not extradite such person in respect of an offence to which this article applies solely on the ground that the person is one of its nationals, shall, at the request of the State Party seeking extradition, be obliged to submit the case without undue delay to its competent authorities for the purpose of prosecution. Those authorities shall take their decisions and conduct their proceedings in the same manner as in the case of any other offence of a comparable nature under the domestic law of that State Party. The States Parties concerned shall cooperate with each other, in particular on procedural and evidentiary aspects, to ensure the efficiency of such prosecution. 12. Whenever a State Party is permitted under its domestic law to extradite or otherwise surrender one of its nationals only upon the condition that the person will be returned to that State Party to serve the sentence imposed as a result of the trial or proceedings for which the extradition or surrender of the person was sought and that State Party and the State Party seeking the extradition of the person agree with this option and other terms that they may deem appropriate, such conditional	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 that the details held on the register are correct at all times.

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
extradition or surrender shall be sufficient to discharge the obligation set forth in paragraph 11 of this article. 13. If extradition, sought for purposes of enforcing a sentence, is refused because the person sought is a national of the requested State Party, the requested State Party shall, if its domestic law so permits and in conformity with the requirements of suc h law, upon application of the requesting State Party, consider the enforcement of the sentence imposed under the domestic law of the requesting State Party or the remainder thereof. 14. Any person regarding whom proceedings are being carried out in connection with any of the offences to which this article applies shall be guaranteed fair treatment at all stages of the proceedings, including enjoyment of all the rights and guarantees provided by the domestic law of the State Party in the territory of which that person is present. 15. Nothing in this Convention shall be interpreted as imposing an obligation to extradite if the requested State Party has substantial grounds for believing that the request has been made for the purpose of prosecuting or punishing a person on account of that person's sex, race, language, religion, nationality, ethnic origin or political opinions, or that compliance with the request would cause prejudice to that person's position for any one of these reasons. 16. States Parties may not refuse a request for extradition on the sole ground that the offence is also considered to involve fiscal matters. 17. Before refusing extradition, the requested State Party shall, where appropriate, consult with the requesting State Party to provide it with ample opportunity to present its opinions and to provide information relevant to its allegation. 18. The requested State Party shall inform the requesting State Party of its decision with regard to the extradition. The requested State Party shall inform the requesting State Party of any reason for refusal of	

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
extradition unless the requested State Party is prevented from doing so by its domestic law or its international legal obligations. 19. Each State 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 United Nations the name and address of an authority responsible for making or receiving requests for extradition or provisional arrest. The Secretary-General shall set up and keep updated a register of authorities so designated by the States Parties. Each State Party shall ensure that the details held in the register are correct at all times. 20. States Parties shall seek to conclude bilateral and multilateral agreements or arrangements to carry out or to enhance the effectiveness of extradition.	
Article 40(1); (2); (4); (7); (21); (22). General principles and procedures relating to mutual legal assistance 1. States Parties shall afford one another the widest measure of mutual legal assistance in investigations, prosecutions and judicial proceedings in relation to the offences established in accordance with this Convention, and for the purposes of the collection of evidence in electronic form of offences established in accordance with this Convention, as well as of serious crimes. 2. Mutual legal assistance shall be afforded to the fullest extent possible under relevant laws, treaties, agreements and arrangements of the requested State Party with respect to investigations, prosecutions and judicial proceedings in relation to the offences for which a legal person may be held liable in accordance with article 18 of this Convention in the requesting State Party. 4. Without prejudice to domestic law, the competent authorities of a State Party may, without prior request, transmit information relating to criminal matters to a competent authority in another State Party where	**BC Article 25 – General principles relating to mutual assistance** 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35. 3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or email, 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,

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
they believe that such information could assist the authority in undertaking or successfully concluding inquiries and criminal proceedings or could result in a request formulated by the latter State Party pursuant to this Convention. 7. Paragraphs 8 to 31 of this article shall apply to requests made pursuant to this article if the States Parties in question are not bound by a treaty on mutual legal assistance. If those States Parties are bound by such a treaty, the corresponding provisions of that treaty shall apply unless the States Parties agree to apply paragraphs 8 to 31 of this article in lieu thereof. States Parties are strongly encouraged to apply the provisions of those paragraphs if they facilitate cooperation. 21. Mutual legal assistance may be refused: (a) If the request is not made in conformity with the provisions of this article; (b) If the requested State Party considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests; (c) If the authorities of the requested State Party would be prohibited by its domestic law from carrying out the action requested with regard to any similar offence, had it been subject to investigation, prosecution or judicial proceedings under their own jurisdiction; (d) If it would be contrary to the legal system of the requested State Party relating to mutual legal assistance for the request to be granted. 22. Nothing in this Convention shall be interpreted as imposing an obligation to afford mutual legal assistance if the requested State Party has substantial grounds for believing that the request has been made for the purpose of prosecuting or punishing a person on account of that person's sex, race, language, religion, nationality, ethnic origin or	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. **BC Article 26 – Spontaneous information** 1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co- operation by that Party under this chapter. 2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them. **Second Protocol Article 10 – Emergency mutual assistance**

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
political opinions, or that compliance with the request would cause prejudice to that person's position for any one of these reasons.	1 Each Party may seek mutual assistance on a rapidly expedited basis where it is of the view that an emergency exists. A request under this article shall include, in addition to the other contents required, a description of the facts that demonstrate that there is an emergency and how the assistance sought relates to it. 2 A requested Party shall accept such a request in electronic form. It may require appropriate levels of security and authentication before accepting the request. 3 The requested Party may seek, on a rapidly expedited basis, supplemental information in order to evaluate the request. The requesting Party shall provide such supplemental information on a rapidly expedited basis. 4 Once satisfied that an emergency exists and the other requirements for mutual assistance have been satisfied, the requested Party shall respond to the request on a rapidly expedited basis. 5 Each Party shall ensure that a person from its central authority or other authorities responsible for responding to mutual assistance requests is available on a twenty-four hour, seven-day-a-week basis for the purpose of responding to a request under this article. 6 The central authority or other authorities responsible for mutual assistance of the requesting and requested Parties may mutually determine that the results of the execution of a request under this article, or an advance copy thereof, may be provided to the requesting Party through a channel other than that used for the request. 7 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, Article 27, paragraphs 2.b and 3 to 8, and Article 28, paragraphs 2 to 4, of the Convention shall apply to this article. 8 Where such a treaty or arrangement exists, this article shall be supplemented by the provisions of such treaty or arrangement unless

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
	the Parties concerned mutually determine to apply any or all of the provisions of the Convention referred to in paragraph 7 of this article, in lieu thereof. 9 Each Party may, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, declare that requests may also be sent directly to its judicial authorities, or through the channels of the International Criminal Police Organization (INTERPOL) or to its 24/7 point of contact established under Article 35 of the Convention. 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. Where a request is sent directly to a judicial authority of the requested Party and that authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform the requesting Party directly that it has done so.
Article 41. 24/7 network 1. Each State Party shall designate a point of contact available 24 hours a day, 7 days a week, in order to ensure the provision of immediate assistance for the purpose of specific criminal investigations, prosecutions or judicial proceedings concerning offences established in accordance with this Convention, or for the collection, obtaining and preservation of evidence in electronic form for the purposes of paragraph 3 of this article and in relation to the offences established in accordance with this Convention, as well as to serious crime. 2. The Secretary-General of the United Nations shall be notified of such point of contact and keep an updated register of points of contact designated for the purposes of this article and shall annually circulate to the States Parties the updated list of contact points.	**BC Article 35 – 24/7 Network** 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects. 2

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
3. Such assistance shall include facilitating or, if permitted by the domestic law and practice of the requested State Party, directly carrying out the following measures: (a) The provision of technical advice; (b) The preservation of stored electronic data pursuant to articles 42 and 43 of this Convention, including, as appropriate, information about the location of the service provider, if known to the requested State Party, to assist the requesting State Party in making a request; (c) The collection of evidence and the provision of legal information; (d) The locating of suspects; or (e) The provision of electronic data to avert an emergency. 4. A State Party's point of contact shall have the capacity to carry out communications with the point of contact of another State Party on an expedited basis. If the point of contact designated by a State Party is not part of that State Party's authority or authorities responsible for mutual legal assistance or extradition, the point of contact shall ensure that it is able to coordinate with that authority or those authorities on an expedited basis. 5. Each State Party shall ensure that trained and equipped personnel are available to ensure the operation of the 24/7 network. 6. States Parties may also use and strengthen existing authorized networks of points of contact, where applicable, and within the limits of their domestic laws, including the 24/7 networks for computer-related crime of the International Criminal Police Organization for prompt police-to-police cooperation and other methods of information exchange cooperation.	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. International cooperation for the purpose of expedited	**BC Article 29 – Expedited preservation of stored computer data**

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
preservation of stored electronic data 1. A State Party may request another State Party to order or otherwise obtain, in accordance with article 25 of this Convention, the expeditious preservation of electronic data stored by means of an information and communications technology system located within the territory of that other State Party, and in respect of which the requesting State Party intends to submit a request for mutual legal assistance in the search or similar access, seizure or similar securing, or disclosure of the electronic data. 2. The requesting State Party may use the 24/7 network provided for in article 41 of this Convention to seek information concerning the location of the electronic data stored by means of an information and communications technology system and, as appropriate, information about the location of the service provider. 3. A request for preservation made under paragraph 1 of this article shall specify: (a) The authority seeking the preservation; (b) The offence that is the subject of a criminal investigation, prosecution or judicial proceeding and a brief summary of the related facts; (c) The stored electronic data to be preserved and their relationship to the offence; (d) Any available information identifying the custodian of the stored electronic data or the location of the information and communications technology system; (e) The necessity of the preservation; (f) That the requesting State Party intends to submit a request for mutual legal assistance in the search or similar access, seizure or similar securing, or disclosure of the stored electronic data;	1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data. 2 A request for preservation made under paragraph 1 shall specify: a the authority seeking the preservation; b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; c the stored computer data to be preserved and its relationship to the offence; d any available information identifying the custodian of the stored computer data or the location of the computer system; e the necessity of the preservation; and f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data. 3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation. 4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
(g) As appropriate, the need to keep the request for preservation confidential and not to notify the user. 4. Upon receiving the request from another State Party, the requested State Party shall take all appropriate measures to preserve expeditiously the specified electronic data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition for providing such preservation. 5. A State Party that requires dual criminality as a condition for responding to a request for mutual legal assistance in the search or similar access, seizure or similar securing, or disclosure of stored electronic data may, in respect of offences other than those established in accordance with 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 could not be fulfilled. 6. In addition, a request for preservation may be refused only on the basis of the grounds contained in article 40, paragraph 21 (b) and (c) and paragraph 22, of this Convention. 7. Where the requested State Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting State Party's investigation, it shall promptly so inform the requesting State Party, which shall then determine whether the request should nevertheless be executed. 8. Any preservation effected in response to a request made pursuant to paragraph 1 of this article shall be for a period of not less than 60 days, in order to enable the requesting State 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.	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. 7 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
9. Before the expiry of the preservation period in paragraph 8 of this article, the requesting State Party may request an extension of the period of preservation.	
Article 43. International cooperation for the purpose of expedited disclosure of preserved traffic data 1. Where, in the course of the execution of a request made pursuant to article 42 of this Convention to preserve traffic data concerning a specific communication, the requested State Party discovers that a service provider in another State Party was involved in the transmission of the communication, the requested State Party shall expeditiously disclose to the requesting State 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 of this article may be refused only on the basis of the grounds contained in article 40, paragraph 21 (b) and (c) and paragraph 22, of this Convention.	**BC 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.
Article 44. Mutual legal assistance in accessing stored electronic data 1. A State Party may request another State Party to search or similarly access, seize or similarly secure, and disclose electronic data stored by means of an information and communications technology system located within the territory of the requested State Party, including electronic data that have been preserved pursuant to article 42 of this Convention. 2. The requested State Party shall respond to the request through the application of relevant international instruments and laws referred to in article 35 of this Convention, and in accordance with other relevant	**BC 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

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
provisions of this chapter. 3. The request shall be responded to on an expedited basis where: (a) There are grounds to believe that the relevant data are particularly vulnerable to loss or modification; or (b) The instruments and laws referred to in paragraph 2 of this article otherwise provide for expedited cooperation.	referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where: a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.
Article 45. Mutual legal assistance in the real-time collection of traffic data 1. States Parties shall endeavour to provide mutual legal assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of an information and communications technology system. Subject to the provisions of paragraph 2 of this article, such assistance shall be governed by the conditions and procedures provided for under domestic law. 2. Each State Party shall endeavour to provide such assistance at least with respect to criminal offences for which the real-time collection of traffic data would be available in a similar domestic case. 3. A request made in accordance with paragraph 1 of this article shall specify: (a) The name of the requesting authority; (b) A summary of the main facts and the nature of the investigation, prosecution or judicial proceeding to which the request relates; (c) The electronic data in relation to which the collection of the traffic data is required and their relationship to the offence;	**BC Article 33 – Mutual Assistance regarding 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.

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
(d) Any available data that identify the owner or user of the data or the location of the information and communications technology system; (e) Justification for the need to collect the traffic data; (f) The period for which traffic data are to be collected and a corresponding justification of its duration.	
Article 46. Mutual legal assistance in the interception of content data States Parties shall endeavour to provide mutual legal assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of an information and communications technology system, to the extent permitted under treaties applicable to them or under their domestic laws.	**BC 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 47. Law enforcement cooperation 1. States Parties shall cooperate closely with one another, consistent with their respective domestic legal and administrative systems, to enhance the effectiveness of law enforcement action to combat the offences established in accordance with this Convention. States Parties shall, in particular, take effective measures: (a) To enhance and, where necessary, to establish channels of communication between their competent authorities, agencies and services, taking into account existing channels, including those of the International Criminal Police Organization, in order to facilitate the secure and rapid exchange of information concerning all aspects of the offences established in accordance with this Convention, including, if the States Parties concerned deem it appropriate, links with other criminal activities;	**Second Protocol Article 12 – Joint investigation teams and joint investigations** 1 By mutual agreement, the competent authorities of two or more Parties may establish and operate a joint investigation team in their territories to facilitate criminal investigations or proceedings, where enhanced coordination is deemed to be of particular utility. The competent authorities shall be determined by the respective Parties concerned. 2 The procedures and conditions governing the operation of joint investigation teams, such as their specific purposes; composition; functions; duration and any extension periods; location; organisation; terms of gathering, transmitting and using information or evidence; terms of confidentiality; and terms for the involvement of the participating authorities of a Party in investigative activities taking place in another Party's territory, shall be as agreed between those competent authorities.

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
(b) To cooperate with other States Parties in conducting inquiries with respect to offences established in accordance with this Convention concerning: (i) The identity, whereabouts and activities of persons suspected of involvement in such offences or the location of other persons concerned; (ii) The movement of proceeds of crime or property derived from the commission of such offences; (iii) The movement of property, equipment or other instrumentalities used or intended for use in the commission of such offences; (c) To provide, where appropriate, necessary items or data for analytical or investigative purposes; (d) To exchange, where appropriate, information with other States Parties concerning specific means and methods used to commit the offences established in accordance with this Convention, including the use of false identities, forged, altered or false documents and other means of concealing activities, as well as cybercrime tactics, techniques and procedures; (e) To facilitate effective coordination between their competent authorities, agencies and services and to promote the exchange of personnel and other experts, including, subject to bilateral agreements or arrangements between the States Parties concerned, the posting of liaison officers; (f) To exchange information and coordinate administrative and other measures taken, as appropriate, for the purpose of early identification of the offences established in accordance with this Convention. 2. With a view to giving effect to this Convention, States Parties shall consider entering into bilateral or multilateral agreements or	3 A Party may declare at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance, or approval that its central authority must be a signatory to or otherwise concur in the agreement establishing the team. 4 Those competent and participating authorities shall communicate directly, except that Parties may mutually determine other appropriate channels of communication where exceptional circumstances require more central coordination. 5 Where investigative measures need to be taken in the territory of one of the Parties concerned, participating authorities from that Party may request their own authorities to take those measures without the other Parties having to submit a request for mutual assistance. Those measures shall be carried out by that Party's authorities in its territory under the conditions that apply under domestic law in a national investigation. 6 Use of information or evidence provided by the participating authorities of one Party to participating authorities of other Parties concerned may be refused or restricted in the manner set forth in the agreement described in paragraphs 1 and 2. If that agreement does not set forth terms for refusing or restricting use, the Parties may use the information or evidence provided: a for the purposes for which the agreement has been entered into; b for detecting, investigating and prosecuting criminal offences other than those for which the agreement was entered into, subject to the prior consent of the authorities providing the information or evidence. However, consent shall not be required where fundamental legal principles of the Party using the information or evidence require that it disclose the information or evidence to protect the rights of an accused person in criminal proceedings. In that case, those authorities

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
arrangements on direct cooperation between their law enforcement agencies and, where such agreements or arrangements already exist, amending them. In the absence of such agreements or arrangements between the States Parties concerned, the States Parties may consider this Convention to be the basis for mutual law enforcement cooperation in respect of the offences established in accordance with this Convention. Whenever appropriate, States Parties shall make full use of agreements or arrangements, including international or regional organizations, to enhance the cooperation between their law enforcement agencies. **Article 48. Joint investigations** States Parties shall consider concluding bilateral or multilateral agreements or arrangements whereby, in relation to offences established in accordance with this Convention that are the subject of criminal investigations, prosecutions or judicial proceedings in one or more States, the competent authorities concerned may establish joint investigative bodies. In the absence of such agreements or arrangements, joint investigations may be undertaken by agreement on a case-by-case basis. The States Parties involved shall ensure that the sovereignty of the State Party in whose territory such investigations are to take place is fully respected.	shall notify the authorities that provided the information or evidence without undue delay; or c to prevent an emergency. In that case, the participating authorities that received the information or evidence shall notify without undue delay the participating authorities that provided the information or evidence, unless mutually determined otherwise. In the absence of an agreement described in paragraphs 1 and 2, joint investigations may be undertaken under mutually agreed terms on a case-by-case basis. This paragraph applies whether or not there is a mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the Parties concerned.
Articles 50. International cooperation for the purposes of confiscation 1. A State Party that has received a request from another State Party having jurisdiction over an offence established in accordance with this Convention for the confiscation of proceeds of crime, property, equipment or other instrumentalities referred to in article 31, paragraph 1, of this Convention situated in its territory shall, to the greatest extent possible within its domestic legal system: (a) Submit the request to its competent authorities for the purpose of obtaining an order of confiscation and, if such an order is granted, give effect to it; or	

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
(b) Submit to its competent authorities, with a view to giving effect to it to the extent requested, an order of confiscation issued by a court in the territory of the requesting State Party in accordance with article 31, paragraph 1, of this Convention insofar as it relates to proceeds of crime, property, equipment or other instrumentalities situated in the territory of the requested State Party. 2. Following a request made by another State Party having jurisdiction over an offence established in accordance with this Convention, the requested State Party shall take measures to identify, trace and freeze or seize proceeds of crime, property, equipment or other instrumentalities referred to in article 31, paragraph 1, of this Convention for the purpose of eventual confiscation to be ordered either by the requesting State Party or, pursuant to a request under paragraph 1 of this article, by the requested State Party. 3. The provisions of article 40 of this Convention are applicable, mutatis mutandis, to this article. In addition to the information specified in article 40, paragraph 15, of this Convention, requests made pursuant to this article shall contain: (a) In the case of a request pertaining to paragraph 1 (a) of this article, a description of the property to be confiscated, including, to the extent possible, the location, and where relevant, the estimated value of the property and a statement of the facts relied upon by the requesting State Party sufficient to enable the requested State Party to seek the order under its domestic law; (b) In the case of a request pertaining to paragraph 1 (b) of this article, a legally admissible copy of an order of confiscation upon which the request is based issued by the requesting State Party, a statement of the facts and information as to the extent to which execution of the order is requested, a statement specifying the measures taken by the requesting State Party to provide adequate notification to	

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
bona fide third parties and to ensure due process, and a statement that the confiscation order is final; (c) In the case of a request pertaining to paragraph 2 of this article, a statement of the facts relied upon by the requesting State Party and a description of the actions requested and, where available, a legally admissible copy of an order on which the request is based. 4. The decisions or actions provided for in paragraphs 1 and 2 of this article shall be taken by the requested State Party in accordance with and subject to the provisions of its domestic law and its procedural rules or any bilateral or multilateral treaty, agreement or arrangement to which it may be bound in relation to the requesting State Party. 5. Each State Party shall furnish copies of its laws and regulations that give effect to this article and of any subsequent changes to such laws and regulations or a description thereof to the Secretary-General of the United Nations. 6. If a State Party elects to make the taking of the measures referred to in paragraphs 1 and 2 of this article conditional on the existence of a relevant treaty, that State Party shall consider this Convention the necessary and sufficient treaty basis. 7. Cooperation under this article may also be refused or provisional measures may be lifted if the requested State Party does not receive sufficient and timely evidence or if the property is of a de minimis value. 8. Before lifting any provisional measure taken pursuant to this article, the requested State Party shall, wherever possible, give the requesting State Party an opportunity to present its reasons in favour of continuing the measure. 9. The provisions of this article shall not be construed as prejudicing the rights of bona fide third parties. 10. States Parties shall consider concluding bilateral or multilateral treaties, agreements or	

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
arrangements to enhance the effectiveness of international cooperation undertaken pursuant to this article.	
Article 51. Special cooperation Without prejudice to its domestic law, each State Party shall endeavour to take measures to permit it to forward, without prejudice to its own criminal investigations, prosecutions or judicial proceedings, information on proceeds of offences established in accordance with this Convention to another State Party without prior request, when it considers that the disclosure of such information might assist the receiving State Party in initiating or carrying out criminal investigations, prosecutions or judicia l proceedings or might lead to a request by that State Party under article 50 of this Convention	
Article 52. Return and disposal of confiscated proceeds of crime or property 1. Proceeds of crime or property confiscated by a State Party pursuant to article 31 or 50 of this Convention shall be disposed of by that State Party in accordance with its domestic law and administrative procedures. 2. When acting on a request made by another State Party in accordance with article 50 of this Convention, States Parties shall, to the extent permitted by domestic law and if so requested, give priority consideration to returning the confiscated proceeds of crime or property to the requesting State Party so that it can give compensation to the victims of the crime or return such proceeds of crime or property to their prior legitimate owners. 3. When acting on a request made by another State Party in accordance with articles 31 and 50 of this Convention, a State Party may, after due consideration has been given to compensation of victims, give special consideration to concluding agreements or arrangements on:	

UN Cybercrime Convention	Budapest Convention ("BC") and Second Additional Protocol ("Second Protocol")
(a) Contributing the value of such proceeds of crime or property or funds derived from the sale of such proceeds of crime or property or a part thereof to the account designated in accordance with article 56, paragraph 2 (c), of this Convention, and to intergovernmental bodies specializing in the fight against cybercrime; (b) Sharing with other States Parties, on a regular or case-by-case basis, such proceeds of crime or property, or funds derived from the sale of such proceeds of crime or property, in accordance with its domestic law or administrative procedures. 4. Where appropriate, unless States Parties decide otherwise, the requested State Party may deduct reasonable expenses incurred in investigations, prosecutions or judicial proceedings leading to the return or disposition of confiscated property pursuant to this article.	