

**WRITTEN CONTRIBUTION FROM THE EUROPEAN UNION AND ITS MEMBER STATES<sup>1</sup> FOR A UNITED NATIONS CONVENTION ON COUNTERING THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES FOR CRIMINAL PURPOSES**

*(Disclaimer)* This contribution is without prejudice to any future contributions that the European Union and its Member States may make during the course of future discussions, including on the present chapters.

Although the issue of the collection of electronic evidence will only be discussed at a later stage of the process, this document contains proposals on that matter in Articles 3(b) and 13(2b). The EU and its Member States remain open to discuss such a collection of electronic evidence for any type of crime, not just cyber-related crimes in order to promote international cooperation under the Convention. This would only be possible if the Convention provides for appropriate safeguards.

**CHAPTER I - GENERAL PROVISIONS**

*Article 1*

*Statement of purpose*

Whilst ensuring a high level of protection of human rights and fundamental freedoms, the purposes of this Convention are:

- a) To promote and strengthen measures to prevent and combat cybercrime more efficiently and effectively,
- b) To promote and facilitate international cooperation,
- c) To ensure a high level of protection of victims' rights and
- d) To support capacity building and technical assistance in the fight against cybercrime.

*Article 2*

*Use of terms*

For the purpose of this Convention:

- a) "Central authority" shall mean the authority or authorities designated for sending and answering requests for mutual assistance, the execution of such request or their transmission to the authorities competent for their execution;

---

<sup>1</sup> Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden.

- b) “Cybercrime” shall mean, for the purpose of this Convention, the conduct as defined in Articles 5 to 10 of this Convention;
- c) “Competent authority” shall mean 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 Convention with respect to specific criminal investigations or proceedings;
- d) “Computer system” shall mean any device or a group of inter-connected or related devices, one or more of which, pursuant to a programme, performs automatic processing of data;
- e) “Computer data“ shall mean any representation of facts, information or concepts in a form suitable for processing in a computer system, including a programme suitable to cause a computer system to perform a function;
- f) “Personal data” shall mean information relating to an identified or identifiable natural person;
- g) “Regional economic integration organisation“ shall mean an organisation 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;
- h) “Service provider“ shall mean:
  - a) Any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
  - b) Any other entity that processes or stores computer data on behalf of such communication service or users of such service;
- i) “Subscriber data” shall mean 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 communication equipment and the site of its installation, available on the basis of the service agreement or arrangement;
- j) "Traffic data" shall mean 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, data, size, duration, or type of underlying service;
- k) "Without right" shall mean conduct referred to in Articles 5 to 10 of this Convention that is not authorised by the owner or by another right holder of the computer system or of part of it, or not permitted under domestic law.

### *Article 3*

#### *Scope of applications*

This Convention shall apply, except as otherwise stated herein, to:

- a) The prevention, investigation and prosecution of criminal offences established in accordance with articles 5 to 10 of this Convention, and
- b) The collection of evidence in electronic form of a criminal offence established in accordance with articles 5 to 10 of this Convention on the basis of the measures set out in Chapter III of this Convention.
- c) The provision and conduct of technical assistance and capacity building on matters covered by this Convention.

### *Article 4*

#### *Effects of the Convention*

1. If two or more States Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in the future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where States Parties establish their future relations in respect of the matters dealt with in the present

Convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.

2. With respect to States Parties that are member of a regional economic integration organisation, those States Parties may, in their mutual relations, apply the rules of that regional economic integration organisation governing the matters dealt with in this Convention.
3. Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party under international law, in particular human rights law.

## **CHAPTER II – CRIMINALISATION AND LAW ENFORCEMENT**

### *Article 5*

#### *Illegal access*

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, the access to the whole or any part of a computer system without right where committed by infringing a security measure.
2. A State Party may require that the offence be committed 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 6*

#### *Illegal interception*

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, 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.
2. A State Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

### *Article 7*

#### *Illegal data interference*

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.
2. A State Party may require that the conduct described in paragraph 1 result in serious harm.

#### *Article 8*

##### *Illegal system interference*

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

#### *Article 9*

##### *Misuse of devices*

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, 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 Articles 5 through 8 of this Convention ;
    - 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 5 through 8 of this Convention; 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 5 through 8 of this Convention. A State Party may require 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 5 through 8 of this Convention, such as for the authorised testing or protection of a computer system.

3. Each State Party may not apply paragraph 1 of this article, provided that it does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

#### *Article 10*

##### *Attempt and aiding and abetting*

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 5 to 9 of this Convention.
2. Each State Party may adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 5 to 9 of this Convention.

#### *Article 11*

##### *Liability of legal persons*

1. Each State Party shall adopt such legislative and other measures as may be necessary, consistent with its legal principles, to ensure that legal persons can be held liable for a criminal offence established in accordance with Articles 5 to 10 of this Convention.
2. Subject to the legal principles of the Party, the liability of a legal person 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.

#### *Article 12*

##### *Prosecution, adjudication and sanctions*

1. Each State Party shall make the commission of an offence established in accordance with articles 5 to 10 of this Convention liable to effective, proportionate and dissuasive sanctions for both natural and legal persons.
2. Each State Party shall endeavour to ensure that any discretionary legal powers under its domestic law relating to the prosecution of persons for offences covered by this

Convention are exercised to maximize the effectiveness of law enforcement measures in respect of those offences and with due regard to the need to deter the commission of such offences.

3. Each State Party shall develop and maintain an effective and rule of law-based national criminal justice system that can ensure that any person prosecuted for offences covered by this Convention is brought to justice whilst ensuring full protection of human rights and fundamental freedoms, including the right to a fair trial and the rights of the defence.

### **CHAPTER III – CRIMINAL PROCEDURES AND LAW ENFORCEMENT**

#### *Article 13*

##### *Scope of procedural measures*

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.
2. 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 Articles 5 through 10 of this Convention; and
  - b) The collection of evidence in electronic form of a criminal offence established in accordance with Articles 5 through 10 of this Convention.

#### *Article 14*

##### *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 adequate and full protection of human rights and fundamental freedoms, in line with international human rights standards including rights arising pursuant to obligations it has undertaken under the 1948 Universal Declaration of Human Rights, the 1966 United Nations International Covenant on Civil and Political Rights, the 1984 Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, the 1989 Convention on the Rights of the Child, the Optional Protocol to the Convention on the

Rights of the Child on the sale of children, child prostitution and child pornography and other international human rights instruments, and which shall incorporate the principles of proportionality, legality and necessity and the protection of privacy and personal data.

2. Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.
3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, each State Party shall consider the impact of the powers and procedures in this chapter upon the rights, responsibilities and legitimate interests of third parties.

#### *Article 15*

##### *Expedited preservation of stored computer data*

1. Each State Party shall adopt 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 State 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 State Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.
4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

## *Article 16*

### *Production order*

1. Each State Party shall adopt measures as may be necessary to empower its competent authorities to order:
  - a) a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and
  - b) a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.
2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

## *Article 17*

### *Search and seizure of stored computer data*

1. Each State Party shall adopt measures as may be necessary to empower its competent authorities to search or similarly access:
  - a) a computer system or part of it and computer data stored therein; and
  - b) a computer-data storage medium in which computer data may be stored in its territory
2. Each State Party shall adopt 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 State 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) a seize or similarly secure a computer system or part of it or a computer-data storage medium;

- b) make and retain a copy of those computer data;
  - c) maintain the integrity of the relevant stored computer data;
  - d) render inaccessible or remove those computer data in the accessed computer system.
4. Each 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 computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.
5. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

#### *Article 18*

#### *Jurisdiction*

1. Each State Party shall adopt such measures as may be necessary to establish jurisdiction over the offence established in accordance with Articles 5 to 10 of this Convention when:
- a) The offence is committed in the territory of that State Party,
  - b) The offence is committed on board a vessel that is flying the flag of that State Party or an aircraft registered under the laws of that State Party at the time to offence is committed, or
  - c) The offence is committed by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.
2. State Party may also establish its jurisdiction over any such offence when:
- a) The offence is committed against a national of that State Party;
  - b) The offence is committed by a national of that State Party or a stateless person who has his or her habitual residence in its territory.
3. Each State Party may also adopt such measures as may be necessary to establish its jurisdiction over the offences covered by this Convention when the alleged offender is present in its territory and it does not extradite him or her, solely on the basis of his or her nationality, after a request for extradition.

4. If a State Party exercising its jurisdiction under paragraph 1 or 2 of this article has been notified, or has otherwise learned, that one or more 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.
5. Without prejudice to norms of general international law, this Convention does not exclude the exercise of any criminal jurisdiction established by a State Party in accordance with its domestic law.

#### *Article 19*

##### *Assistance to and protection of victims*

1. Each State Party shall take appropriate measures within its means to provide assistance and protection to victims of offences established in accordance with Articles 5 to 10 of this Convention.
  2. Each State Party shall establish appropriate procedures to provide access to compensation for victims of offences established in accordance with Articles 5 to 10 of this Convention.
  3. Each State Party shall, subject to its domestic law, enable views and concerns of victims to be presented and considered at appropriate stages of criminal proceedings against offenders in a manner not prejudicial to the rights of the defence.
-