Project on Cybercrime
www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Version November 2008
[Reformat in May 2011]

Cybercrime legislation – country profile

STATE OF BRUNEI DARUSSALEM

This profile has been prepared within the framework of the Council of Europe's capacity building projects on cybercrime in view of sharing information and assessing the current state of implementation of the Convention on Cybercrime under domestic legislation. It does not necessarily reflect official positions of the country covered or of the Council of Europe.

Comments may be sent to:

Economic Crime Division
Directorate General of Human Rights and Legal Affairs
Council of Europe, Strasbourg, France

Tel: +33-3-9021-4506
Fax: +33-3-9021-5650
Email: alexander.seger@coe.int
www.coe.int/cybercrime

Country:	**State of Brunei Darussalem**
Signature of Convention:	No
Ratification/accession:	No
Provisions of the Convention	***Corresponding provisions/solutions in national legislation*** *(pls quote or summarise briefly; pls attach relevant extracts as an appendix)*
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data": For the purposes of this Convention: a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs	**Art.2 (Interpretation) and Art. 18(5) of Computer Misuse Act 2007 of Brunei Darussalam.** "Computer" means an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices,

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	performing logical, arithmetic or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include:- a) a similar device which is non-programmable or which does not contain any data storage facility; or b) such other device as the Minister may, by notification in the Gazette, prescribe; "Computer output" means a statement or representation (whether in written, printed, pictorial, graphical or other form0 purporting to be a statement or representation of fact:– a) produced by a computer; or b) accurately translated from a statement or representation so produced; "computer program" means data representing instructions or statement that, when executed in a computer, causes the computer to perform a function; "computer services" includes computer time, data processing and storage or retrieval of data; "data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer; **BROADCASTING ACT (CAP. 180)** **BROADCASTING (CLASS LICENSE) NOTIFICATION 2001** **2. " Internet Service Provider"** means any of the following persons:- a) an Internet Access Service Provider licensed under section 3 of the Telecommunications Act (CAP.54) b) a Localised Internet Service Reseller; or c) a Non-localised Internet Service Reseller; **There is no specific definition of "traffic data" in any of our legislations.**

Chapter II – Measures to be taken at the national level ***Section 1 – Substantive criminal law***	
Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems	
Article 2 – Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when 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.	**Computer Misuse Act 2007 of Brunei Darussalam.** **3.** (1) Subject to subsection (2), any person who knowingly causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer is guilty of an offence and liable on conviction to a fine not exceeding five thousand dollars, imprisonment for a term not exceeding two years or both and in the case of a second or subsequent conviction, to a fine not exceeding ten thousand dollars, imprisonment for a term not exceeding three years or both. (2) If any damage is caused as a result of an offence under this section, the person convicted of the offence is liable to a fine not exceeding fifty thousand dollars, imprisonment for a term not exceeding seven years or both. (3) For the purposes of this section, it is immaterial that the act in question was not directed at — *(a)* any particular program or data; *(b)* a program or data of any kind; or *(c)* a program or data held in any particular computer.
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 committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	**Computer Misuse Act 2007 of Brunei Darussalam.** **6.** (1) Subject to subsection (2), any person who knowingly- b) intercepts or causes to be intercepted without authority, directly or indirectly, any function of a computer by means of an electromagnetic, acoustic, mechanical or other device; is guilty of an offence and is liable on conviction to a fine not exceeding ten thousand dollars, imprisonment for a term not exceeding three years or both, and in the case of a second or subsequent conviction, to a fine not exceeding twenty thousand dollars or imprisonment for a term not exceeding five years or both.

	9. (1) Where access to any protected computer is obtained in the course of the commission of an offence under section 3,5,6 or 7, the person convicted of such offence is in lieu of the punishments respectively prescribed in those sections liable on conviction to a fine not exceeding one hundred thousand dollars, imprisonment for a term not exceeding twenty years or both.
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.	**Computer Misuse Act 2007 of Brunei Darussalam.** **2.** (7) For the purpose of this Order, a modification of the contents of any computer takes place if, by the operation of any function of that computer or any other computer – a) any program or data held in that computer is altered or erased; b) any program or data is added to its contents; and any act which contributes towards causing such modification shall be regarded as causing it. **5.** (1) Subject to subsection (2), any person who does any act which he knows will cause an unauthorised modification of the contents of any computer is guilty of an offence and is liable on conviction to a fine not exceeding ten thousand dollars, imprisonment for a term not exceeding three years or both, and in the case of a second or subsequent conviction, to a fine not exceeding twenty thousand dollars, imprisonment for a term not exceeding five years or both. (2) If any damage is caused as a result of an offence under this section, the person convicted of the offence is liable to a fine not exceeding fifty thousand dollars, imprisonment for a term not exceeding seven years or both. (3) For the purposes of this section, it is immaterial that the act in question was not directed at — *(a)* any particular program or data; *(b)* a program or data of any kind; or *(c)* a program or data held in any particular computer.

	(4) For the purposes of this section, it is immaterial whether an unauthorised modification is, or is intended to be, permanent or temporary. **7.** (1) (b) **Unauthorised obstruction of use of computer.** (1) Any person who knowingly and without authority or lawful excuse — (b) impedes or prevents access to, or impairs the usefulness or effectiveness of, any program or data stored in a computer, is guilty of an offence and liable on conviction to a fine not exceeding ten thousand dollars, imprisonment for a term not exceeding three years or both, and in the case of a second or subsequent conviction, to a fine not exceeding twenty thousand dollars, imprisonment for a term not exceeding five years or both. **9.** (1) **Enhanced punishment for offences involving protected computers.** Where access to any protected computer is obtained in the course of the commission of an offence under section 3, 5, 6 or 7, the person convicted of such offence is in lieu of the punishments respectively prescribed in those sections, liable on conviction to a fine not exceeding one hundred thousand dollars, imprisonment for a term not exceeding twenty years or both.
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	**Computer Misuse Act 2007 of Brunei Darussalam.** **2.** (7) For the purpose of this Order, a modification of the contents of any computer takes place if, by the operation of any function of that computer or any other computer – c) any act which impairs the normal operation of any computer, and any act which contributes towards causing such modification shall be regarded as causing it. **7.** (1) Any person who knowingly and without authority or lawful excuse — *(a)* interferes with, or interrupts or obstructs the lawful use of, a computer; or *(b)* impedes or prevents access to, or impairs the usefulness or effectiveness of, any program or data stored in a computer, is guilty of an offence and liable on

	conviction to a fine not exceeding ten thousand dollars, imprisonment for a term not exceeding three years or both, and in the case of a second or subsequent conviction, to a fine not exceeding twenty thousand dollars, imprisonment for a term not exceeding five years or both. (2) If any damage is caused as a result of an offence under this section, the person convicted of the offence is liable to a fine not exceeding fifty thousand dollars, imprisonment for a term not exceeding seven years or both. **9.** (1) **Enhanced punishment for offences involving protected computers.** Where access to any protected computer is obtained in the course of the commission of an offence under section 3, 5, 6 or 7, the person convicted of such offence is in lieu of the punishments respectively prescribed in those sections, liable on conviction to a fine not exceeding one hundred thousand dollars, imprisonment for a term not exceeding twenty years or both.
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	**Computer Misuse Act 2007 of Brunei Darussalam.** **8. Unauthorised disclosure of access code.** (1) Any person who knowingly and without authority discloses any password, access code or other means of gaining access to any program or data held in any computer is guilty of an offence if he did so — (a) for any wrongful gain; (b) for any unlawful purpose; or (c) knowing that it is likely to cause wrongful loss to any person. (2) Any person guilty of an offence under subsection (1) is liable on conviction to a fine not exceeding ten thousand dollars, imprisonment for a term not exceeding three years or both, and in the case of a second or subsequent conviction, to a fine not exceeding twenty thousand dollars, imprisonment for a term not exceeding five years or both. **Electronic Transaction Order 2000** **25.**

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.	
Title 2 – Computer-related offences	
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	**Computer Misuse Act 2007 of Brunei Darussalam.** **5. Unauthorised modification of computer material.** (1) Subject to subsection (2), any person who does any act which he knows will cause an unauthorised modification of the contents of any computer is guilty of an offence and is liable on conviction to a fine not exceeding ten thousand dollars, imprisonment for a term not exceeding three years or both, and in the case of a second or subsequent conviction, to a fine not exceeding twenty thousand dollars, imprisonment for a term not exceeding five years or both. (2) If any damage is caused as a result of an offence under this section, the person convicted of the offence is liable to a fine not exceeding fifty thousand dollars, imprisonment for a term not exceeding seven years or both. (3) For the purposes of this section, it is immaterial that the act in question was not directed at — (a) any particular program or data; (b) a program or data of any kind; or (c) a program or data held in any particular computer. (4) For the purposes of this section, it is immaterial whether an unauthorised modification is, or is intended to be, permanent or temporary. **9. Enhanced punishment for offences involving protected computers** (1) Where access to any protected computer is obtained in the course of the commission of an offence under section 3, 5, 6 or 7, the person convicted of such offence is in lieu of the punishments respectively prescribed in those

	sections, liable on conviction to a fine not exceeding one hundred thousand dollars, imprisonment for a term not exceeding twenty years or both. (2) For the purposes of subsection (1), a computer shall be treated as a "protected computer" if the person committing the offence knew, or ought reasonably to have known, that the computer, program or data was used directly in connection with or necessary for — (a) the security, defence or international relations of Brunei Darussalam; (b) the existence or identity of a confidential source of information relating to the enforcement of a criminal law; (c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure; or (d) the protection of public safety, including systems related to essential emergency services, such as police and medical services. (3) For the purposes of any prosecution under this section, it shall be presumed, until the contrary is proved, that the accused had the requisite knowledge referred to in subsection (2) if there was, in respect of the computer, program or data, an electronic or other warning exhibited to the accused stating that unauthorised access to that computer program or data will attract an enhanced penalty under this section.
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.	**Computer Misuse Act 2007 of Brunei Darussalam.** **4.** (1) Any person who causes a computer to perform any function for the purpose of securing access to any program or data held in a computer with intent to commit an offence to which this section applies is guilty of an offence. (2) This section applies to an offence involving property, fraud, dishonesty or which causes bodily harm and which is punishable on conviction with imprisonment for a term of not less than two years. (3) Any person guilty of an offence under this section is liable on conviction to a fine not exceeding fifty thousand dollars, imprisonment for a term not exceeding ten years or both. (4) For the purposes of this section, it is immaterial whether — *(a)* the access referred to in subsection (1) was authorised or unauthorised;

	(b) the offence to which this section applies was committed at the same time when the access was secured or at any other time. **9. Enhanced punishment for offences involving protected computers** (1) Where access to any protected computer is obtained in the course of the commission of an offence under section 3, 5, 6 or 7, the person convicted of such offence is in lieu of the punishments respectively prescribed in those sections, liable on conviction to a fine not exceeding one hundred thousand dollars, imprisonment for a term not exceeding twenty years or both. (2) For the purposes of subsection (1), a computer shall be treated as a "protected computer" if the person committing the offence knew, or ought reasonably to have known, that the computer, program or data was used directly in connection with or necessary for — (a) the security, defence or international relations of Brunei Darussalam; (b) the existence or identity of a confidential source of information relating to the enforcement of a criminal law; (c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure; or (d) the protection of public safety, including systems related to essential emergency services, such as police and medical services. (3) For the purposes of any prosecution under this section, it shall be presumed, until the contrary is proved, that the accused had the requisite knowledge referred to in subsection (2) if there was, in respect of the computer, program or data, an electronic or other warning exhibited to the accused stating that unauthorised access to that computer program or data will attract an enhanced penalty under this section.
Title 3 – Content-related offences	
Article 9 – Offences related to child pornography 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a	There is no separate legal provision concerning Child Pornography, but we mention the ' Undesirable Publications Act ', which constitutes an Act to prevent the importation, distribution or reproduction of undesirable publications and for purposes connected therewith. For Art. 9(1/a-c) can be used Art. 4(1) and for Art. 9(1/e) - Art. 4(2) of Undesirable Publications Act of Brunei Darussalam.

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. 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.	**Section 292 of Penal Code of Brunei Darussalam.** **Sale etc. of obscene articles.** **292.** (1) For the purposes of this section and section 293 an article shall be deemed to be obscene if its effect or (where the article comprises 2 or more distinct items) the effect of any one of its items is, if taken as a whole, such as to tend to deprave and corrupt persons who, having regard to all relevant circumstances, are likely (or would have been likely but for the lawful seizure of the article) to read, see or hear the matter contained or embodied in it. (2) In this section, "article" means any description of article containing or embodying matter to be read or looked at or both, any sound record, and any film, video cassette, photographic negative or other record of a picture. (3) Whoever — *(a)* sells, lets to hire, distributes, publicly exhibits or in any manner puts into circulation, or for purposes of sale, hire distribution, public exhibition or circulation makes, produces or has in his possession any obscene article; or *(b)* imports, exports or conveys any obscene article for any of the purposes aforesaid, or knowing or having reason to believe that such article will be sold, let to hire, distributed or publicly exhibited or in any manner put into circulation; or *(c)* takes part in or receives profits from any business in the course of which he knows or has reason to believe that any such obscene articles are, for any of the purposes aforesaid, made produced, purchased, kept, imported, exported, conveyed, publicly exhibited or in any manner put into circulation; or *(d)* advertises or makes known by any means whatsoever that any person is engaged or is ready to engage in any act which is an offence under this section or that any such obscene article can be produced from or through any person; or *(e)* offers or attempts to do any act which is an offence under this section, *Exception* — This section does not extend to any book, pamphlet, writing, drawing or painting kept or used *bona fide* for religious purposes or any representation sculptured, engraved, painted or otherwise represented on or in any temple.

	Sale etc. of obscene articles to person under the age of 20 years. **293.** Whoever sells, lets to hire, distributes, exhibits or circulates to any person under the age of 20 years any obscene articles, or offers or attempts so to do, shall be guilty of an offence: Penalty, a fine of not less than $1,000 and not more than $10,000 and imprisonment which may extend to 3 years and in the case of a second or subsequent conviction, a fine of not less than $3,000 and not more than $50,000 and imprisonment which may extend to 5 years. *[S 12/97]* At present there is no specific law which covers crimes against a child using the Internet.
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that	**Copyright Order 2000.** **Offences** **Criminal liability for making or dealing with Infringing articles, etc.** **204.** (1) A person commits an offence who, without the licence of the copyright owner — *(a)* makes for sale or hire; *(b)* imports otherwise than for his private and domestic use; *(c)* communicates the work to the public; *(d)* in the course of a business, possesses, with a view to committing any act infringing the copyright; *(e)* in the course of a business — (i) sells or lets for hire; (ii) offers or exposes for sale or hire; (iii) exhibits in public; or (iv) distributes; or *(f)* otherwise than in the course of a business, distributes to such an extent as to prejudicially affect the owner of the copyright, an article which is, and which he knows or has reason to believe is, an infringing copy of a copyright work.

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.	(2) A person commits an offence who *(a)* makes an article specifically designed or adapted for making copies of a particular copyright work; or *(b)* has such an article in his possession, if he knew or had reason to believe that it was to be used to make infringing copies for sale or hire or for use in the course of a business. (3) Where copyright is infringed, otherwise than by reception of a broadcast or cable programme — *(a)* by the public performance of a literary, dramatic or musical work; or *(b)* by the playing or showing in public of a sound recording or film, any person who caused the work to be so performed, played or shown is guilty of an offence if he knew or had reason to believe that copyright would be infringed. (4) Sections 106, 107 and 108 do not apply to proceedings for an offence under this section; but without prejudice to their application in proceedings for an order under section 209. (5) A person guilty of an offence under paragraphs *(a)* or *(b),* subparagraph (iv) of paragraph *(e)*, or paragraph *(f)*, of subsection (1) is liable on conviction to imprisonment for a term not exceeding two years, a fine or both. (6) A person guilty of any other offence under this section is liable on conviction to imprisonment for a term not exceeding six months, a fine not exceeding five thousand dollars or both. **Criminal liability for making, etc., illicit recordings.** **205.** (1) A person commits an offence who, without sufficient consent — *(a)* makes for sale or hire; *(b)* imports otherwise than for his private and domestic use; *(c)* makes available to the public; *(d)* in the course of a business, possesses, with a view to

	committing any act infringing the rights conferred by this Part; or *(e)* in the course of a business — (i) sells or lets for hire; (ii) offers or exposes for sale or hire; or (iii) distributes, a recording which is, and which he knows or has reason to believe is, an illicit recording. (2) A person commits an offence who causes a recording of a performance made without sufficient consent to be — *(a)* shown or played in public; or *(b)* broadcast or included in a cable programme service, thereby infringing any of the rights conferred by this Part, if he knew or had reason to believe that those rights are thereby infringed. (3) In subsections (1) and (2), "sufficient consent" means — *(a)* in the case of a qualifying performance, the consent of the performer; and *(b)* in the case of a non-qualifying performance subject to an exclusive recording contract — (i) for the purpose of paragraph *(a)* of subsection (1), the consent of the performer or the person having recording rights; and (ii) for the purpose of paragraphs *(b)*, *(c)* and *(d)* of subsection (1), and of subsection (2), the consent of the person having recording rights. The references in this subsection to the person having recording rights are to the person having those rights at the time the consent was given or, if there is more than one such person, to all of them. (4) No offence is committed under subsections (1) or (2) by the commission of an act which under any provision of the Second Schedule may be done without infringing the rights conferred by this Part.

	(5) A person guilty of an offence under paragraphs *(a)* or *(b)*, or subparagraph (iii) of paragraph *(e)*, of subsection (1) is liable on conviction to imprisonment for a term not exceeding two years, a fine or both. (6) A person guilty of any other offence under this section is liable on conviction to imprisonment for a term not exceeding six months, a fine not exceeding five thousand dollars or both. **Application of Chapter 96 in enforcement.** **206.** (1) Section 30 of the Merchandise Marks Act applies to the enforcement of sections 204 and 205 of this Order as to the enforcement of that Act. (2) Any law which authorises the disclosure of information for the purpose of facilitating the enforcement of the Merchandise Marks Act shall apply as if sections 204 and 205 of this Order were contained in that Act, and as if the powers of any person in relation to the enforcement of that section were powers under that Act. **False representation of authority to give consent.** **207.** (1) It is an offence for a person to falsely represent that he is authorised by any person to give consent for the purpose of this Part in relation to a performance, unless he believes on reasonable grounds that he is so authorised. (2) A person guilty of an offence under subsection (1) is liable on conviction to imprisonment for a term not exceeding six months, a fine not exceeding five thousand dollars or both. **Offences committed by partnerships and bodies corporate.** **208.** (1) Where an offence under this Order committed by a body corporate is proved to have been committed with the consent or connivance of, or to be attributable to any act or default on the part of, a director, manager, secretary or other similar officer of that body, or of a person purporting to act in any such capacity, he, as well as the body corporate, is also guilty of that offence and liable to be proceeded against and punished accordingly

	(2) Where a partnership is guilty of an offence under this Order, every partner, other than a partner who is proved to have been ignorant of or to have attempted to prevent the commission of the offence, is also guilty of the offence and liable to be proceeded against and punished accordingly (3) In relation to a body corporate whose affairs are managed by its members, "director", in subsection (1), means any member of the body corporate. In addition to the **Copyright Order, 2000,** Brunei Darussalam has also enacted the following additional legislation relating to intellectual property. **Trade Marks Act (Cap. 98 of the Laws of Brunei Darussalam);** **Industrial Designs Order, 2000;** **Inventions Act (Cap. 72 of the Laws of Brunei Darussalam);**
Title 5 – Ancillary liability and sanctions	
Article 11 – Attempt and aiding or abetting 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention. 3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	**Computer Misuse Act 2007** **10.** (1) Any person who abets the commission of or who attempts to commit or does any act preparatory to or in furtherance of the commission of any offence under this Order is shall be guilty of that offence and liable on conviction to the punishment provided for the offence.

Article 12 – Corporate liability 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a a power of representation of the legal person; b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority. 3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	**Electronic Transaction Order 2000** **49.**
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.	**Computer Misuse Act 2007** **2 – 10** **2. Interpretation.** (1) In this Order, unless the context otherwise requires — "computer" means an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include — (a) a similar device which is non-programmable or which does not contain any data storage facility; or (b) such other device as the Minister may, by notification in the Gazette, prescribe; "computer output" means a statement or representation (whether in written, printed, pictorial, graphical or other form) purporting to be a statement

	or representation of fact — (a) produced by a computer; or (b) accurately translated from a statement or representation so produced; "computer program" means data representing instructions or statements that, when executed in a computer, causes the computer to perform a function; "computer service" includes computer time, data processing and the storage or retrieval of data; "damage" means, except for the purposes of section 13, any impairment to a computer or the integrity or availability of data, a program or system, or information, that — (a) causes loss aggregating at least ten thousand dollars in value, or such other amount as the Minister may by notification in the Gazette prescribe, except that any loss incurred or accrued more than one year after the date of the offence in question shall not be taken into account; (b) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment or care of one or more persons; (c) causes or threatens physical injury or death to any person; or (d) threatens public health or public safety; "data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer; "electronic, acoustic, mechanical or other device" means any device or apparatus that is used or is capable of being used to intercept any function of a computer; "function" includes logic, control, arithmetic, deletion, storage and retrieval, read and write, and communication or telecommunication to, from or within a computer; "intercept", in relation to a function of a computer, includes listening to or recording a function of a computer, or acquiring the substance, meaning or purport thereof; "Minister" means the Minister of Finance; "output" has the same meaning as "computer output"; "program" has the same meaning as "computer program". (2) For the purposes of this Order, a person secures access to any program or data held in a computer if by causing a computer to perform any function he —

	(a) alters or erases the program or data; (b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held; (c) uses it; or (d) causes it to be output from the computer in which it is held (whether by having it displayed or in any other manner), and references to access to a program or data (and to an intent to secure such access) shall be read accordingly. (3) For the purposes of paragraph (c) of subsection (2), a person uses a program if the function he causes the computer to perform — (a) causes the program to be executed; or (b) is itself a function of the program. (4) For the purposes of paragraph (d) of subsection (2), the form in which any program or data is output (and in particular whether or not it represents a form in which, in the case of a program, it is capable of being executed or, in the case of data, it is capable of being processed by a computer) is immaterial. (5) For the purposes of this Order, access of any kind by any person to any program or data held in a computer is unauthorised or done without authority if — (a) he is not himself entitled to control access of the kind in question to the program or data; and (b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled. (6) A reference in this Order to any program or data held in a computer includes a reference to any program or data held in any removable storage medium which is for the time being in the computer; and a computer is to be regarded as containing any program or data held in any such medium. (7) For the purposes of this Order, a modification of the contents of any computer takes place if, by the operation of any function of that computer or any other computer — (a) any program or data held in that computer is altered or erased; (b) any program or data is added to its contents; or (c) any act which impairs the normal operation of any computer, and any act which contributes towards causing such a modification shall be regarded as

causing it.
(8) Any modification referred to in subsection (7) is unauthorised if —
(a) the person whose act causes it is not himself entitled to determine whether the modification should be made; and
(b) he does not have consent to the modification from any person who is so entitled.
(9) A reference in this Order to a program includes a reference to part of a program.

3. Unauthorised access to computer material.

(1) Subject to subsection (2), any person who knowingly causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer is guilty of an offence and liable on conviction to a fine not exceeding five thousand dollars, imprisonment for a term not exceeding two years or both and in the case of a second or subsequent conviction, to a fine not exceeding ten thousand dollars, imprisonment for a term not exceeding three years or both.
(2) If any damage is caused as a result of an offence under this section, the person convicted of the offence is liable to a fine not exceeding fifty thousand dollars, imprisonment for a term not exceeding seven years or both.
(3) For the purposes of this section, it is immaterial that the act in question was not directed at —
(a) any particular program or data;
(b) a program or data of any kind; or
(c) a program or data held in any particular computer.

4. Access with intent to commit or facilitate commission of offence.

(1) Any person who causes a computer to perform any function for the purpose of securing access to any program or data held in a computer with intent to commit an offence to which this section applies is guilty of an offence.
(2) This section applies to an offence involving property, fraud, dishonesty or

	which causes bodily harm and which is punishable on conviction with imprisonment for a term of not less than two years. (3) Any person guilty of an offence under this section is liable on conviction to a fine not exceeding fifty thousand dollars, imprisonment for a term not exceeding ten years or both. (4) For the purposes of this section, it is immaterial whether — (a) the access referred to in subsection (1) was authorised or unauthorised; (b) the offence to which this section applies was committed at the same time when the access was secured or at any other time. **5. Unauthorised modification of computer material.** (1) Subject to subsection (2), any person who does any act which he knows will cause an unauthorised modification of the contents of any computer is guilty of an offence and is liable on conviction to a fine not exceeding ten thousand dollars, imprisonment for a term not exceeding three years or both, and in the case of a second or subsequent conviction, to a fine not exceeding twenty thousand dollars, imprisonment for a term not exceeding five years or both. (2) If any damage is caused as a result of an offence under this section, the person convicted of the offence is liable to a fine not exceeding fifty thousand dollars, imprisonment for a term not exceeding seven years or both. (3) For the purposes of this section, it is immaterial that the act in question was not directed at — (a) any particular program or data; (b) a program or data of any kind; or (c) a program or data held in any particular computer. (4) For the purposes of this section, it is immaterial whether an unauthorised modification is, or is intended to be, permanent or temporary. **6. Unauthorised use or interception of computer service.** (1) Subject to subsection (2), any person who knowingly — (a) secures access without authority to any computer for the purpose of obtaining, directly or indirectly, any computer service;

	(b) intercepts or causes to be intercepted without authority, directly or indirectly, any function of a computer by means of an electromagnetic, acoustic, mechanical or other device; or (c) uses or causes to be used, directly or indirectly, the computer or any other device for the purpose of committing an offence under paragraph (a) or (b), is guilty of an offence and is liable on conviction to a fine not exceeding ten thousand dollars, imprisonment for a term not exceeding three years or both, and in the case of a second or subsequent conviction, to a fine not exceeding twenty thousand dollars or imprisonment for a term not exceeding five years or both. (2) If any damage is caused as a result of an offence under this section, the person convicted of the offence is liable to a fine not exceeding fifty thousand dollars, imprisonment for a term not exceeding seven years or both. (3) For the purposes of this section, it is immaterial that an unauthorised access or interception was not directed at — (a) any particular program or data; (b) a program or data of any kind; or (c) a program or data held in any particular computer. **7. Unauthorised obstruction of use of computer.** (1) Any person who knowingly and without authority or lawful excuse — (a) interferes with, or interrupts or obstructs the lawful use of, a computer; or (b) impedes or prevents access to, or impairs the usefulness or effectiveness of, any program or data stored in a computer, is guilty of an offence and liable on conviction to a fine not exceeding ten thousand dollars, imprisonment for a term not exceeding three years or both, and in the case of a second or subsequent conviction, to a fine not exceeding twenty thousand dollars, imprisonment for a term not exceeding five years or both. (2) If any damage is caused as a result of an offence under this section, the person convicted of the offence is liable to a fine not exceeding fifty thousand dollars, imprisonment for a term not exceeding seven years or both. **8. Unauthorised disclosure of access code.**

(1) Any person who knowingly and without authority discloses any password, access code or other means of gaining access to any program or data held in any computer is guilty of an offence if he did so —
(a) for any wrongful gain;
(b) for any unlawful purpose; or
(c) knowing that it is likely to cause wrongful loss to any person.
(2) Any person guilty of an offence under subsection (1) is liable on conviction to a fine not exceeding ten thousand dollars, imprisonment for a term not exceeding three years or both, and in the case of a second or subsequent conviction, to a fine not exceeding twenty thousand dollars, imprisonment for a term not exceeding five years or both.

9. Enhanced punishment for offences involving protected computers.

(1) Where access to any protected computer is obtained in the course of the commission of an offence under section 3, 5, 6 or 7, the person convicted of such offence is in lieu of the punishments respectively prescribed in those sections, liable on conviction to a fine not exceeding one hundred thousand dollars, imprisonment for a term not exceeding twenty years or both.
(2) For the purposes of subsection (1), a computer shall be treated as a "protected computer" if the person committing the offence knew, or ought reasonably to have known, that the computer, program or data was used directly in connection with or necessary for —
(a) the security, defence or international relations of Brunei Darussalam;
(b) the existence or identity of a confidential source of information relating to the enforcement of a criminal law;
(c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure; or
(d) the protection of public safety, including systems related to essential emergency services, such as police and medical services.
(3) For the purposes of any prosecution under this section, it shall be presumed,

	until the contrary is proved, that the accused had the requisite knowledge referred to in subsection (2) if there was, in respect of the computer, program or data, an electronic or other warning exhibited to the accused stating that unauthorised access to that computer program or data will attract an enhanced penalty under this section. **Electronic Transaction Order 2000** **25** **48 (2)**
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the	**Computer Misuse Act 2007.** **12.** Notwithstanding the provisions of any written law to the contrary, a Court of a Magistrate shall have jurisdiction to try any offence under this Order and to award the full punishment for any offence. **14.** Nothing in this Order shall prohibit a police officer, any person authorised in writing by the Commissioner of Police under subsection (1) of section 18 or any other duly authorized law enforcement officer from lawfully conducting investigations pursuant to his powers conferred under any written law. **18.** (1) A police officer or any person authorised in writing by the Commissioner of Police shall — *(a)* be entitled at any time to — (i) have access to and inspect and check the operation of any computer to which this section applies; (ii) use or cause to be used any such computer to search any data contained in or available to such computer; or (iii) have access to any information, code or technology which has the capability of retransforming or unscrambling encrypted data contained

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	or available to such computer into readable and comprehensible format or text for the purpose of investigating any offence under this Order or any other offence which has been disclosed in the course of the lawful exercise of the powers under this section; *(b)* be entitled to require — (i) the person by who or on whose behalf the police officer or investigation officer has reasonable cause to suspect any computer to which this section applies is or has been used; or (ii)any person having charge of, or otherwise concerned with the operation of, such computer, to provide him with such reasonable technical and other assistance as he may require for the purposes of paragraph *(a)*; or *(c)* be entitled to require any person in possession of decryption information to grant him access to such decryption information necessary to decrypt data required for the purpose of investigating any such offence. (2) This section applies to a computer which a police officer or any person authorized in writing by the Commissioner of Police has reasonable cause to suspect is or has been in use in connection with any offence under this Order or any other offence which has been disclosed in the course of the lawful exercise of the powers under this section. (3) The powers referred to in sub-paragraphs (ii) and (iii) of paragraph *(a)* and in paragraph *(c)* of subsection (1) shall not be exercised except with the consent of the Public Prosecutor. (4) Any person who obstructs the lawful exercise of the powers under paragraph *(a* of subsection (1) or who fails to comply with a request under paragraph *(b)* or *(c)* of subsection (1) is guilty of an offence and liable on conviction to a fine not exceeding ten thousand dollars, imprisonment for a term not exceeding three years or both. (5) For the purposes of this section — "decryption information" means information or technology that enables a person to readily retransform or unscramble encrypted data from its unreadable and

	incomprehensible format to its plain text version; "encrypted data" means data which has been transformed or scrambled from its plain text version to an unreadable or incomprehensible format, regardless of the technique utilised for such transformation or scrambling and irrespective of the medium in which such data occurs or can be found for the purposes of protecting the content of such data; "plain text version" means original data before it has been transformed or scrambled to an unreadable or incomprehensible format. **19.** Any police officer may arrest without warrant any person reasonably suspected of committing an offence under this Order.
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 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.	Not Applicable
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	None

expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 17 – Expedited preservation and partial disclosure of traffic data 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.	None

Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	For Art. 18 (1/a)- Art. 18(1/b/ii, 1/c) of **Computer Misuse Act 2007 of Brunei Darussalam.** **18.** (1) A police officer or any person authorised in writing by the Commissioner of Police shall — (b) be entitled to require — (ii)any person having charge of, or otherwise concerned with the operation of, such computer, to provide him with such reasonable technical and other assistance as he may require for the purposes of paragraph (a); or (c) be entitled to require any person in possession of decryption information to grant him access to such decryption information necessary to decrypt data required for the purpose of investigating any such offence.
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 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	**For Art. 19(1/a)- Art. 18(1/a/i-ii) of Computer Misuse Act 2007 of Brunei Darussalam.** **18.** (1) A police officer or any person authorised in writing by the Commissioner of Police shall — (a) be entitled at any time to — (i) have access to and inspect and check the operation of any computer to which this section applies; (ii) use or cause to be used any such computer to search any data contained in or available to such computer; or **Electronic Transaction Order 2000**

grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**14** **53**
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.	None

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.	
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. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	None

Section 3 – Jurisdiction	
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	**Computer Misuse Act 2007** **11.** (1) Subject to subsection (2), this Order shall have effect in relation to any person, whatever his nationality, whether within or outside Brunei Darussalam; and where an offence under this Order has been committed by any person outside Brunei Darussalam, he may be dealt with as if the offence had been committed within Brunei Darussalam. (2) For the purposes of subsection (1), this Order shall apply if, for the offence in question — *(a)* the accused was in Brunei Darussalam at the material time; or *(b)* the computer, program or data was in Brunei Darussalam at the material time.
Chapter III – International co-operation	
Article 24 – Extradition 1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. b Where a different minimum penalty is to be applied under an	**Extradition Order 2006**

arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply. 2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them. 3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article. 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party. 7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party	

shall ensure	
Article 25 – General principles relating to mutual assistance 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35. 3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.	**Mutual Assistance in Criminal Matters Order 2004** **3.** The object of this Order is to facilitate the provision and obtaining, by Brunei Darussalam, of international assistance in criminal matters, including – *(a)* the obtaining of evidence, documents, articles or other things; *(b)* the making of arrangements for persons, including detained persons to give evidence or assist investigations; *(c)* the confiscation of property in respect of offences; *(d)* the service of documents; *(e)* the identification and location of persons; *(f)* the execution of requests for search and seizure; *(g)* providing originals or certified copies of relevant documents and records, including government, bank, financial, corporate or business records. Government records may be provided in accordance with whether or not they are in the public domain within the laws of Brunei Darussalam; and *(h)* any other type of assistance that is not contrary to the laws of Brunei Darussalam.

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.	
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times. 3 Mutual assistance requests under this article shall be executed in	**Mutual Assistance in Criminal Matter Order 2004** **4.** (1) This Order applies to any foreign country subject to – *(a)* any mutual assistance treaty between that country and Brunei Darussalam and *(b)* any multilateral mutual assistance treaty being a treaty to which that country and Brunei Darussalam are parties to. (2) This Order does not prevent the provision or obtaining of international assistance in criminal matters to or from the International Criminal Police (Interpol) or any other international organisation. (3) This Order does not prevent the provision or obtaining of international assistance in criminal matters to or from any foreign country other than assistance of a kind that may be provided or obtained under this Order. **Requests to be made to Attorney General.** **21.** (1) Every request by a foreign country for assistance in a criminal matter pursuant to this Part of this Order shall be made to the Attorney General by a person or authority responsible for transmitting or receiving such request.

accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party. 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities. 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary. 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly. 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party. b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol). c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.	(2) If a foreign country makes a request to a court in Brunei Darussalam for international assistance in a criminal matter - (a) the court must refer the request to the Attorney-General; and (b) the request is then taken, for the purposes of this Order, to have been made to the Attorney-General. **Requests for assistance.** **22.** (1) If a foreign country requests assistance under this Part, the Attorney General must consider the following matters in order to decide whether the request should be dealt with - (a) if there is in force a treaty, memorandum of understanding or other agreement between Brunei Darussalam and that country under which that country has agreed to provide assistance in criminal matters in Brunei Darussalam; (b) if the request is made in accordance with a convention to which Brunei Darussalam and that country are parties which provide for the convention be used as a basis of providing assistance in criminal matters; (c) if (a) and (b) are not applicable, (i) any assurances given by that country that it will entertain a similar request by Brunei Darussalam for assistance in criminal matters; (ii) the seriousness of the offence to which the request relates; (iii) the object of this Order as specified in section 3 and (iv) any other matters that the Attorney General considers relevant. (2) If, after considering those matters, the Attorney General decides that the request should be dealt with under this Part, the Attorney General may deal with that request accordingly. **Form of request.** **23.** Every request by a foreign country for assistance under this Part of this Order shall - (a) be made in writing or by any means capable of producing a written record and it should be made in English;

d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party. e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.	(b) be made orally only in urgent circumstances but shall be confirmed in writing later; (c) specify the purpose of the request and the nature of the assistance being sought; (d) identify the person, agency or authority that initiated the request; and (e) be accompanied by - (i) a statement from that country that the request is made in respect of a criminal matter within the meaning of this Order; (ii) a description of the nature of the criminal matter and a statement setting out a summary of the relevant facts and laws; (iii) where the request relates to - (A) the location of a person who is suspected to be involved in or has benefited from the commission of an offence; or (B) the tracing of property that is connected with a criminal matter, the name, identity, nationality, location or description of that person, or the location and description of the property, if known, and a statement setting forth the basis for suspecting the matter referred to in sub-paragraph (A) or (B); (iv) a description of the offence to which the criminal matter relates, including its maximum penalty; (v) details of the procedure that that country wishes to be followed by Brunei Darussalam in giving effect to the request, including details of the manner and form in which any information, article or thing is to be supplied to that country pursuant to the request; (vi) a statement setting out the wishes of that country concerning the confidentiality of the request and the reason for those wishes; (vii) details of the period within which that country wishes the request to be met; (viii) if the request involves a person travelling from Brunei

	Darussalam to that country, details of allowances to which the person will be entitled, and of the arrangements for accommodation for the person while he is in that country pursuant to the request; (ix) any other information required to be included with the request under any treaty, memorandum of understanding or other agreement between Brunei Darussalam and that country; and (x) any other information that may assist in giving effect to the request or which is required under the provision of this Order.
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. 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.	
Article 29 – Expedited preservation of stored computer data 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 under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. 5 In addition, a request for preservation may only be refused if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request	

should nevertheless be executed. 4 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.	
Article 30 – Expedited disclosure of preserved traffic data 1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted. 2 Disclosure of traffic data under paragraph 1 may only be withheld if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	
Article 31 – Mutual assistance regarding accessing of stored computer data 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where: a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	**Mutual Assistance in Criminal Matters Order 2004** **Assistance in obtaining evidence in Brunei Darussalam.** **26.** A foreign country may request the Attorney General to assist in arranging - (a) the taking of evidence in Brunei Darussalam; or (b) the production of documents, articles or other things in Brunei Darussalam. **Assistance in the taking of evidence.** **27.** (1) Where, on receipt of a request made under this subsection by a foreign country, the Attorney General is satisfied - (a) that the request relates to a criminal matter in the foreign country; and (b) there are reasonable grounds for believing that the evidence can be taken or, as the case may be, the documents articles or

	other things can be produced in Brunei Darussalam, the Attorney General may by notice in writing, subject to such terms and conditions, authorise a Magistrate to take the evidence before transmitting the evidence to the foreign country. (2) Upon receipt of the notice made under subsection (1), the Magistrate shall - (a) take the evidence of each witness appearing before him.; (b) cause the evidence to be reduced in writing and certify at the end of that writing that the evidence was taken by him; and (c) cause the writing, so certified, to be sent to the Attorney General. (3) The proceedings may be conducted in the presence or absence of the person to whom the criminal matter in the foreign country relates or of his legal representative (if any). (4) If the requesting country has so requested, the Magistrate conducting a proceeding under subsection (2) may permit - (a) any person to whom the proceeding in the requesting country relates or that person's legal representative; or (b) the legal representative of the relevant authority of the requesting country, to examine or cross-examine, including through a live television link from the requesting country, any person giving evidence or producing a document or other article, at the proceeding. (5) The certificate referred to in subsection (2) shall state whether the person to whom the criminal matter in the foreign country relates or his legal representative (if any) was present at the proceedings. (6) The laws for the time being in force with respect to the compelling of persons to attend before a Magistrate, and to give evidence, answer questions and produce documents, upon hearing of a charge against a person for an offence against the law of Brunei Darussalam shall apply, so far as they are capable of application, with respect to the compelling of persons to attend before a Magistrate, and to give evidence, answer questions and produce

	documents, for the purposes of this section. (7) For the purposes of this section, the person to whom the criminal matter in the foreign country relates is competent but not compellable to give evidence. (8) No person who is required under this section to give evidence for the purposes of any criminal matter in a foreign country shall be required to answer any question that the person could not be compelled to answer in those proceedings in that country. (9) A duly certified foreign law immunity certificate is admissible in proceedings under this section as prima facie evidence of the matters stated in the certificate. (10) Evidence taken under this section shall not be admissible in evidence, or otherwise used, for the purposes of any judicial proceedings, disciplinary proceedings, or other proceedings, in Brunei Darussalam except in the prosecution of the person who gave that evidence for the offence of perjury, or contempt of court, in respect of that evidence. **Production orders for criminal matters.** **29.** (1) Where a request is made by a foreign country that any document or other articles in Brunei Darussalam be produced for the purposes of any criminal matter in that country, the Attorney General or a person duly appointed by him may apply to the court for an order under subsection 2. (2) If, on such an application, the court is satisfied that the production of the article or thing is necessary or desirable for the purposes of the foreign criminal matter to which the application relates, it may make an order that the person who appears to the court to be in possession of the article or thing shall - (a) produce the article or thing to an authorised officer for him to take away; or (b) give an authorised officer access to the article or thing, within 7 days of the date of the order or such other period as the court considers appropriate.

	(3) In this section, the documents or other articles produced (a) shall include copies of government records, documents or information which under the laws of Brunei Darussalam are available to the general public; (b) may include at the Attorney General's discretion, the whole, in part or subject to certain conditions, copies of any government records, documents or information which under the law of Brunei Darussalam are not available to the general public. (c) may include at the Court's discretion, items subject to legal privilege (4) The proceedings referred to in subsection (2) may be conducted in the presence or absence of the person to whom the criminal proceedings in the foreign country relates or of his legal representative (if any). (7) No person who is required by an order under this section to produce or make available anything for the purposes of any criminal proceedings in a foreign country shall be required to produce any document or other article that the person could not be compelled to produce in the proceedings in that country. (8) A duly certified foreign law immunity certificate is admissible in proceedings under this section as prima facie evidence as the matters stated in the certificate. (9) Proceedings under subsection (3) shall be heard in camera.
Article 32 – Trans-border access to stored computer data with consent or where publicly available A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	
Article 33 – Mutual assistance in the real-time collection of traffic	

data 1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	
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.	**Mutual Assistance in Criminal Matters Order 2004** **Supplementary provisions regarding production orders.** **31.** (1) Where a court orders a person under section 29 to give an authorised officer access to any article or thing on any premises, it may, on the same or a subsequent application of an authorised officer, order any person who appears to him to be entitled to grant entry to the premises, to allow an authorised officer to enter the premises to obtain access to the article or thing. (2) Where any material to which an order under section 29 relates consists of information contained in or accessible by means of any data equipment - (a) an order under section 29 shall have effect as an order to produce the material in a form which can be taken away and which is visible and legible; and (b) an order under section 29 shall have effect as an order to give access to the material in a form which is visible and legible. (3) A person is not excused from producing or making available any article or thing by an order under section 29 on the ground that - (a) the production or making available of the article or thing will incriminate the person or make the person liable to a penalty; or (b) the production or making available of the article or thing would be in breach of an obligation (whether imposed by law or otherwise) of the person not to disclose the existence of the contents of the article or thing. (4) An order under section 29 shall have effect notwithstanding any

	obligation as to secrecy or other restrictions upon the disclosure of information imposed by statute or otherwise. (5) An authorised officer may photograph or make copies of any article or thing produced or to which access is granted pursuant to an order made under section 29. (6) Where an authorised officer takes possession of any article or thing under an order made under section 29 or takes any photograph or makes any copy of the article or thing under subsection (5), he may retain the article or thing, photograph or copy for a period of up to one month pending a written direction from the Attorney General as to the manner in which the article or thing, photograph or copy is to be dealt with (which may include a direction that the article or thing, photograph or copy be sent to the appropriate authority of the foreign country concerned). (7) Rules of Court under section 55 may provide for - (a) the discharge and variation of orders under section 29; and (b) proceedings relating to such orders. (8) In this section, "data equipment" means any equipment which - (a) automatically processes information; (b) automatically records or stores information; (c) can be used to cause information to be automatically recorded, stored or otherwise processed on other equipment (wherever situated); (d) can be used to retrieve information whether information is recorded or stored in the equipment itself or in other equipment (wherever situated).
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 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis. 3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.	
Article 42 – Reservations By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.	