Council of the European Union

Brussels, 16 July 2025
(OR. en)

11556/25

Interinstitutional File:
2025/0231 (NLE)

CYBER 212
COPEN 211
JAI 1067
COPS 382
RELEX 999
JAIEX 79
TELECOM 244
POLMIL 210
CFSP/PESC 1148
ENFOPOL 269
DATAPROTECT 154

PROPOSAL

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	16 July 2025
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2025) 417 final
Subject:	Proposal for a COUNCIL DECISION on the conclusion, on behalf of the European Union, of the United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes

Delegations will find attached document COM(2025) 417 final.

Encl.: COM(2025) 417 final

EUROPEAN
COMMISSION

Brussels, 16.7.2025
COM(2025) 417 final

2025/0231 (NLE)

Proposal for a

COUNCIL DECISION

on the conclusion, on behalf of the European Union, of the United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

Objectives of the proposal

The present proposal aims to obtain from the Council of the European Union ('the Council') the authorisation for the European Commission ('the Commission') to conclude the United Nations Convention against Cybercrime ('the Convention') on behalf of the European Union[(1)].

This proposal complements a separate proposal from the Commission for a Decision of the Council authorising the Commission to sign the Convention on behalf of the European Union. Together, these proposals follow up on the Commission's commitment in ProtectEU – the European Internal Security Strategy.[(2)]

Cybercrime continues to be a growing threat to the security of citizens and businesses in the European Union (EU).[(3)] According to the Europol Internet Organised Crime Threat Assessment, in the last 10 years, the threats posed by cybercrime have evolved dynamically in terms of volume, intensity and harm potential.[(4)] Cybercriminals leverage emerging technologies such as Artificial Intelligence (AI) for attack automation, social engineering, and bypassing security measures, making cyber-attacks more scalable and efficient. Economic recession, geopolitical instability and widening global inequality have increased incentives for individuals to engage in financially motivated cybercrime.[(5)] Cyber-enabled offences, such as online fraud and child sexual abuse, continue growing in size and scale. €1.03 trillion are estimated to have been lost globally in 2024 due to online fraud.[(6)] Global reports of child sexual abuse have increased from 1 million in 2010 to almost 36 million in 2023, of which 1.3 million in the EU.[(7)]

Cybercrime is a global and borderless phenomenon and stepping up international cooperation to fight cybercrime has been a priority for countries around the world for over a decade. In particular, the borderless nature of the internet makes cybercrime investigations almost always cross-border in nature, thus requiring close cooperation between authorities in different countries. In recent years, the number of countries with which cooperation is required has been growing, as cybercriminals hide in convenient jurisdictions around the globe to commit their attacks on the EU and its partner countries.

Electronic evidence is increasingly important for criminal investigations, both into online and traditional crimes, like drugs trafficking, which often leave online traces as criminals plan and coordinate their activities online and on applications. As a result, a Commission

---

(1) The text of the Convention will be annexed to the proposal for a Council Decision authorising Member States to ratify, in the interest of the Union, the Convention.

(2) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on ProtectEU: a European Internal Security Strategy; COM/2025/148 final.

(3) In 2023, ransomware attacks, child sexual exploitation (CSE) and online fraud remained the most threatening manifestations of cybercrime in the European Union (EU). Some cybercriminals targeting the EU were based within the EU, while others preferred to operate from abroad, concealing their illicit operations and funds in third countries. Internet Organised Crime Threat Assessment (IOCTA) 2024.

(4) Internet Organised Crime Threat Assessment (IOCTA) 2024.

(5) Serious and Organised Crime Threat Assessment (SOCTA) 2025.

(6) Global State of Scams Report 2025 (GASA).

(7) National Centre for Missing and Exploited Children, https://www.missingkids.org/cybertiplinedata.

survey found that, already in 2018, law enforcement and judicial authorities needed access to electronic evidence in at least 85 % of criminal investigations, including cybercrime.[8] Evidence of any criminal offence is increasingly held in electronic form by service providers in foreign jurisdictions. At least 55 % of investigations include a request for cross-border access to evidence.[9] An effective criminal justice response requires appropriate measures to obtain such evidence to uphold the rule of law.

Therefore, actions to improve the sharing of electronic evidence for criminal investigations are being undertaken at national, at EU[10] and at the international levels.

The Convention is part of these actions. It provides common rules at global level to enhance cooperation on cybercrime and the collection of evidence in electronic form for the purpose of criminal investigations or proceedings, creating a basis for cooperation with many countries with whom neither the EU nor its Member States have agreements in place, while ensuring respect for the EU's laws and values. It is compatible with and complementary to existing EU and international instruments.

Background

The 2001 Council of Europe Convention on Cybercrime (the 'Budapest Convention')[11] is the first international treaty on cybercrime. It facilitates the fight against criminal offences making use of computer networks. The Budapest Convention is open to Member States of the Council of Europe, and non-members upon invitation. To date, it has 80 States Parties, including 26 European Union Member States. The Second Additional Protocol[12] to the Budapest Convention, includes updated rules on the exchange of electronic evidence.[13]

The European Union and its Member States are also parties to two of the main United Nations criminal justice instruments of almost universal adoption, the United Nations Convention against Organised Crime (UNTOC)[14] and the United Nations Convention against Corruption (UNCAC).[15]

---

(8) SWD(2018) 118 final.

(9) SWD(2018) 118 final.

(10) Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (OJ L 191, 28.7.2023, p. 118–180, ELI: http://data.europa.eu/eli/reg/2023/1543/oj) and Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings, (OJ L 191, 28.7.2023, p. 181–190, ELI: http://data.europa.eu/eli/dir/2023/1544/oj).

(11) CETS No. 185.

(12) CETS No. 224.

(13) The Council adopted decisions authorising Member States to sign and ratify the Second Additional Protocol in the interest of the EU: Council Decision (EU) 2022/722 of 5 April 2022 authorising Member States to sign, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (OJ L 134, 11.5.2022, p. 15–20, ELI: http://data.europa.eu/eli/dec/2022/722/oj) and Council Decision (EU) 2023/436 of 14 February 2023 authorising Member States to ratify, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence; (OJ L 63, 28.2.2023, p. 48–53, ELI: http://data.europa.eu/eli/dec/2023/436/oj).

(14) Doc. A/55/383. The EU signed UNTOC on 12 December 2000 and ratified it on 21 May 2004 and also ratified its protocols on smuggling and trafficking in human beings. See 2004/579/EC: Council Decision of 29 April 2004 on the conclusion, on behalf of the European Community, of the United Nations Convention Against Transnational Organised Crime (OJ L 261, 6.8.2004, p. 69–69, ELI: http://data.europa.eu/eli/dec/2004/579/oj); 2006/616/EC: Council Decision of 24 July 2006 on the

The provisions of the new Convention are aligned and compatible with these three established and widely adopted international instruments.

The rise of information technology and the rapid development of new telecommunication and computer network systems and the use and abuse of technologies for criminal purposes have also featured on the agenda of the United Nations (UN). On 21 December 2010, the UN General Assembly adopted Resolution 65/230 requesting the Commission on Crime Prevention and Criminal Justice (CCPCJ) to establish an open-ended intergovernmental expert group ('the IEG') to conduct a comprehensive study on the problem of cybercrime.

The UN General Assembly adopted resolution 73/187 of 17 December 2018 on 'Countering the use of information and communications technologies for criminal purposes.' On 27 December 2019, the UN General Assembly adopted a second Resolution, 74/247, on the same topic, establishing an open-ended ad hoc intergovernmental committee of experts ('the AHC') to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes. The Resolution specified that the AHC was to take into full consideration existing international instruments and efforts at the national, regional and international levels on combating the use of information and communications technologies for criminal purposes, in particular the work and outcomes of the IEG.

On 24 May 2022, the Council authorised the Commission to participate, on behalf of the European Union, in the negotiations on the Convention.[16] The Commission participated in line with the Decision of the Council and was guided by the negotiating directives set out therein. The Commission was supported by the European External Action Service (EEAS). The Commission consistently consulted the Council's special committee for the negotiations on the Union position and ensured the Convention's compatibility with relevant EU acquis.

In line with the Framework Agreement on relations between the European Parliament and the European Commission,[17] the Commission also kept the European Parliament informed of the negotiations.

The Commission also informed the European Data Protection Supervisor (EDPS) and the European Data Protection Board (EDPB) during and following the conclusion of the negotiations.

---

conclusion, on behalf of the European Community, of the Protocol Against the Smuggling of Migrants by Land, Sea and Air, supplementing the United Nations Convention Against Transnational Organised Crime concerning the provisions of the Protocol, in so far as the provisions of this Protocol fall within the scope of Articles 179 and 181a of the Treaty establishing the European Community (OJ L 262, 22.9.2006, p. 24–33, ELI: http://data.europa.eu/eli/dec/2006/616/oj) and 2006/619/EC: Council Decision of 24 July 2006 on the conclusion, on behalf of the European Community, of the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women And Children, supplementing the United Nations Convention Against Transnational Organised Crime concerning the provisions of the Protocol, in so far as the provisions of the Protocol fall within the scope of Part III, Title IV of the Treaty establishing the European Community (OJ L 262, 22.9.2006, p. 51–58, ELI: http://data.europa.eu/eli/dec/2006/619/oj).

(15) United Nations, Treaty Series, vol. 2349, p. 41; Doc. A/58/422. The EU signed UNCAC on 15 September 2005 and ratified it on 12 November 2008. See 2008/801/EC: Council Decision of 25 September 2008 on the conclusion, on behalf of the European Community, of the United Nations Convention against Corruption (OJ L 287, 29.10.2008, p. 1–110, ELI: http://data.europa.eu/eli/dec/2008/801/oj).

(16) Council Decision (EU) 2022/895 of 24 May 2022 authorising the opening of negotiations on behalf of the European Union for a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, (OJ L 155, 8.6.2022, p. 42–48, ELI: http://data.europa.eu/eli/dec/2022/895/oj).

(17) Reference L 304/47.

The AHC met eight times in formal sessions between 28 February 2022 and 9 August 2024. It also held informal sessions in between and five intersessional sessions for consultations with a diverse range of stakeholders, including global and regional intergovernmental organizations, non-governmental organizations, civil society organizations, academic institutions and the private sector.

On 8 August 2024 the AHC approved by consensus the draft text of the Convention and the draft UN General Assembly resolution accompanying it. The UN General Assembly adopted both documents by consensus on 24 December 2024.[18] The Convention is envisaged to be opened for signature in Hanoi, Vietnam on 25 October 2025, and thereafter at United Nations Headquarters in New York until 31 December 2026.

The Convention will enter into force once 40 States Parties have expressed their consent to be bound by the Convention in accordance with the provisions of Article 65, paragraphs 1 and 2.

In accordance with well-established practice regarding UNTOC and UNCAC, the Convention provides that a regional economic integration organization, such as the European Union can sign and ratify the Convention if at least one of the Member States signs and ratifies it.

Reasons for the proposal

The Convention is in line with the Union's objectives set out in ProtectEU, the 2025 European Internal Security Strategy to tackle crime and facilitate access to digital evidence for all crimes through international instruments such as the Convention. It complements existing EU and international instruments to which the EU and/or its Member States are Parties, such as the Council of Europe Budapest Convention, and thus contributes to the EU's fight against transnational crime.

First, as a UN instrument, the Convention has a wider reach in terms of membership than existing EU and international instruments. In this respect, it is similar to previous UN instruments on cooperation in criminal matters of almost universal adoption, such as UNTOC and UNCAC. It can thus enable enhanced cooperation against cybercrime at a global scale.

Second, the Convention is inspired by the Budapest Convention's criminalisation provisions, which can further enhance cooperation based on a long-standing and tested legal framework. Given its more recent adoption, the Convention also introduces further criminalisation provisions on offences that have seen a drastic increase over the last years: online fraud, the solicitation or grooming to commit a sexual offence against a child, and the non-consensual dissemination of intimate images. These are already criminalised at the EU level but not yet at a global one.

Third, the Convention enables the exchange of electronic evidence between the authorities of its States Parties on forms of serious crimes also on the rise, including offences related to terrorism and transnational organised crime. This limit to serious crimes restricts the use of the mechanism to serious cases only, which helps ensure proportionality. It also prevents overburdening national authorities with requests and reflects the different levels of trust in cooperation that exist at the international level.

Fourth, the Convention supplements existing international instruments, such as the Budapest Convention, by including procedural measures on the protection of victims and witnesses, tools for the recovery of cybercrime proceeds, and international cooperation measures on the transfer of sentenced persons and criminal proceedings, joint investigations and law enforcement cooperation.

---

(18) Resolution adopted by the General Assembly on 24 December 2024; A/RES/79/243.

Fifth, the Convention includes a chapter on technical assistance and capacity building to help developing countries build their capabilities and enable them to contribute to the global fight against cybercrime.

Sixth, the Convention requires States Parties to the Convention to respect human rights, including criminal procedural rights and safeguards (such as the right to a fair trial, the rights of the defence, judicial or other independent review), and the right to the protection of personal data for every measure under the Convention. In view of its universal vocation and acknowledging existing differences in the level of protection of human rights around the world, the Convention includes provisions to exclude its use to commit human rights violations and provide States Parties with unprecedented grounds to refuse cooperating with other Parties in such cases. More information in this regard is provided in the Sections *'Consistency with existing policy provisions in the policy area'*, *'Fundamental rights'* and *'Detailed explanation of the specific provisions of the proposal'* below. These provisions make the Convention the first of its kind with such comprehensive human rights protection and safeguards. Upon its entry into force, the Convention will become a benchmark for future international instruments and will contribute to mainstreaming these human rights safeguards in global cooperation in criminal matters.

- **Consistency with existing policy provisions in the policy area**

The fight against cybercrime is a priority for the European Union as recognised by the Council in its 2024 Strategic guidelines for legislative and operational planning within the area of freedom, security and justice[(19)] and by the Commission's 2025 ProtectEU - European Internal Security Strategy which announces EU action to tackle online crime and to facilitate access to digital evidence for all crimes, including through international instruments for information and evidence exchange, such as the timely signature and conclusion of the Convention.

The Commission recognises the need to further advance and strengthen the capacities of law enforcement and judicial authorities in this field, to develop national cybercrime legislation, where not sufficiently provided. It also acknowledges the need to promote international cooperation in the fight against cybercrime and supports a range of capacity building programmes in a number of countries worldwide, including for developing countries.[(20)] The Commission has supported the work of the IEG, the UN Commission on Crime Prevention and Criminal Justice, the United Nations Office on Drugs and Crime (UNODC), the Committee of the Budapest Convention on Cybercrime and other bodies.

The provisions of the Convention are consistent with EU rules and policies in the areas of judicial cooperation in criminal matters, police cooperation and data protection as well as with relevant bilateral and multilateral agreements to which the European Union is already a Party.

Reservations and notifications

The Convention does not have a provision dedicated to reservations. However, it explicitly provides for reservations in some provisions (Article 11 paragraph 3; Article 23 paragraph 3(a); Article 23 paragraph 3 chausette; Article 42 paragraph 5; Article 63 paragraphs 3 and 4) and implicitly allows other reservations as long as those are in accordance with Article 19 paragraph (c) of the Vienna Convention on the Law of Treaties[(21)] and customary international

(19) Strategic guidelines for legislative and operational planning within the area of freedom, security and justice, 28 November 2024, para. 19.

(20) See for instance the Global Action on Cybercrime Enhanced (GLACY-e), via https://www.coe.int/en/web/cybercrime/glacy-e.

(21) United Nations, Treaty Series, vol. 1155, p. 331

law and hence are not incompatible with the object and purpose of the Convention. Therefore, the Convention allows for significant flexibility regarding reservations. Member States should take a uniform approach to reservations and notifications, as set out in Annex I to this Decision. Reservations and notifications should be compatible with Union and public international law and do not defeat the object and purpose of the Convention. The human rights conditions and safeguards recognised and provided for in this Convention are part of its object and purpose and therefore not open to reservations.

- **Consistency with other Union policies**

The Convention is consistent with relevant European Union rules and policies in the areas which will be covered by it (international cooperation and mutual legal assistance between public authorities of Member States and Member States and third countries as described under Section *'Consistency with existing policy provisions in the policy area'*) and with relevant bilateral and multilateral agreements to which the European Union is already a Party. Other Union policy areas remain unaffected.

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

- **Legal basis**

The proposal is made under Article 218(6) of the Treaty on the Functioning of the European Union (TFEU). Article 218 of the TFEU lays down the procedure for the negotiation and conclusion of agreements between the European Union and third countries or international organisations. In particular, paragraph 6 thereof provides for the Council, on a proposal from the Commission as the negotiator, to adopt a decision authorising the concluding of an agreement on behalf of the European Union.

The substantive legal basis for a decision under Article 218(6) TFEU depends primarily on the objective and content of the envisaged international agreement in respect of which a position is taken on the Union's behalf. If the envisaged international agreement pursues two aims or has two components and if one of those aims or components is identifiable as the main one, whereas the other is merely incidental, the decision under Article 218(6) TFEU must be founded on a single substantive legal basis, namely that required by the main or predominant aim or component.

With regard to an envisaged international agreement that simultaneously pursues a number of objectives, or that has several components, which are inseparably linked without one being incidental to the other, the substantive legal basis of a decision under Article 218(6) TFEU will have to include, exceptionally, the various corresponding legal bases.

As regards matters on the facilitation of the cooperation between judicial or equivalent authorities in relation to proceedings in criminal matters and the enforcement of decisions, the substantive legal basis is Article 82(1) TFEU. As regards the definition of criminal offences in the area of cybercrime, the substantive legal basis is Article 83(1) TFEU. As regards measures concerning law enforcement cooperation on the substantive legal basis is Article 87(2) of the TFEU. As regards the protection of personal data the substantive legal basis is Article 16 TFEU.

- Union competence

The subject matter of the Convention is the fight against cybercrime by way of, *inter alia*, criminalizing certain serious harmful types of conduct and establishing international cooperation to that end, including with regard to electronic evidence. This falls within shared

competence between the Union and the Member States in accordance with Article 4(2)(j) TFEU.

Certain provisions of the Convention, notably the provision on data protection, fall within areas covered to a large extent by common rules that could be affected, or whose scope could be altered, by the Convention. Therefore, as regards such areas and in line with Article 3(2) TFEU, the Union has exclusive external competence for the conclusion of the Convention.

The conclusion of the Convention by the European Commission, in the interest of the Union, may thus take place on the basis of Articles 16, 82(1), (83)(1), 87(1) and 218(6) TFEU.

- **Subsidiarity (for non-exclusive competence)**

Acting at the EU level serves to promote a harmonious application of the provisions of the Convention in EU Member States and ensures its compatibility with existing and future EU instruments. Furthermore, EU action in this area enhances the combined leverage and impact of the EU and its Member States in the mechanisms of implementation of the Convention, such as its Conference of States Parties (Article 57), as well as in the future negotiation of Protocols (Article 62) thereto.

- **Proportionality**

The Union's objectives with regard to this proposal as set out in Section *'Reasons for the proposal'* above can only be achieved by entering into a binding international agreement providing for the necessary cooperation measures while ensuring appropriate protection of fundamental rights. The Convention achieves this objective. The provisions of the Convention are limited to what is necessary to achieve its main objectives and do not encroach on existing EU instruments or international instruments to which the EU is a Party to.

- **Choice of the instrument**

Article 218(6) TFEU provides that the Commission or the High Representative of the Union for Foreign Affairs and Security Policy, depending on the subject matter of the agreement envisaged, shall submit proposals to the Council, which shall adopt a decision authorising the conclusion of an international agreement. Given the subject matter of the Convention, it is appropriate for the Commission to submit a proposal to that effect.

3. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

- **Ex-post evaluations/fitness checks of existing legislation**

Not Applicable

- **Stakeholder consultations**

The Commission published a call for evidence for this initiative on its website on 14 January 2022, which was available for comments for four weeks. The individual responses to the call for evidence were published on the consultation website. These considerations have been taken into account in the preparation of the Commission's proposal for entering into negotiations on the Convention.

To ensure greater transparency of the process, General Assembly Resolution 75/282 setting out the organisational matters concerning the AHC ensured the involvement of representatives of interested global and regional intergovernmental organizations, including representatives of United Nations bodies, specialised agencies and funds, as well as representatives of functional commissions of the Economic and Social Council in the substantive sessions as observers. Furthermore, this Resolution enabled non-governmental organisations (including global and

regional intergovernmental organizations, non-governmental organizations, civil society organizations, academic institutions and the private sector) to register and attend the sessions of the AHC, where they were regularly given the opportunity to present their views during the plenary sessions on the chapters being discussed. Pursuant to this Resolution five intersessional consultation sessions with stakeholders were held. Stakeholders were also able to submit written materials, which were published on the website of the AHC.

The Commission, in its role as negotiator, also regularly engaged with diverse stakeholders throughout the negotiations and considered their contributions.

- **Collection and use of expertise**

During the negotiations, the Commission, as the Union representative, consulted the Council's special committee for the negotiations in line with the Decision of the Council of 22 May 2022 authorising the Commission to participate in the negotiations on behalf of the Union. As UN Members, EU Member States were able to attend in all negotiation sessions. The Commission consulted their representatives on its formulation of the Union's position throughout the negotiations. The Commission also regularly consulted stakeholders (see Section *'Stakeholder consultations'* above).

- **Impact assessment**

Relevant impacts are presented in this explanatory memorandum.

- **Regulatory fitness and simplification**

The Convention may have implications for certain public authorities and categories of service providers. Due to more international cooperation on the sharing of electronic evidence to combat cybercrime and cyber-enabled offences, there could be an increase of the number of requests for electronic evidence that EU Member States' central authorities for mutual legal assistance may receive from their counterparts in other States Parties to the Convention and then relay, subject to all applicable national rules and procedures, to service providers established in their State. At the same time, the legal framework for international cooperation on cybercrime that the Convention establishes at a global scale, as well as the safeguards and conditions it contains, will provide service providers with more legal certainty as regards the requests for access to data they may face pursuant to cooperation between states on criminal matters.

- **Fundamental rights**

The Convention provides safeguards allowing EU Member States to comply with human rights obligations under international, EU and national law. These safeguards also prevent the abuse of this UN instrument by States Parties to commit or legitimise human rights violations.

The provisions of the Convention cover procedural and international cooperation measures in criminal matters, such as extradition, mutual legal assistance and the exchange of electronic evidence, that would interfere with fundamental rights, such as the rights to liberty and to being protected from inhuman and degrading treatment, and the rights to privacy and to the protection of personal data. The Convention follows a rights-based approach and provides for both horizontal and context specific robust human rights conditions and safeguards that are in line with existing international instruments on human rights and on cooperation in criminal matters. The Convention also caters to those human rights risks that are inherent to the fight against cybercrime and the nature of the internet. As regards the human rights obligations of its States Parties, the Convention repeatedly refers to "international human rights law". This wide expression covers both international instruments and customary international law on

human rights, and thus ensures the widest possible application of international human rights obligations to all future Parties to the Convention, regardless of their adherence to specific international human rights instruments.

Article 6 provides an overarching requirement for States Parties to respect their obligations under international human rights law when implementing the Convention. It also excludes any of its Parties from interpreting the Convention as permitting them to use this legal instrument to suppress human rights or fundamental freedoms. To underscore this obligation in the digital context in which this Convention operates, Article 6 paragraph 2 also includes a non-exhaustive list of those human rights and fundamental freedoms that are more prone to be affected by potential abuses in the digital sphere, including the freedoms of expression, conscience, opinion, religion or belief, peaceful assembly and association. This horizontal provision, due to its placement and nature, applies to the whole Convention and forms part of the object and purpose of the Convention.

Article 21, paragraph 4, is also a horizontal provision concerning the harmonisation of the prosecution, adjudication and sanction of the Convention's offences. It requires States Parties to ensure that any person prosecuted for offences established in accordance with this Convention enjoys all rights and guarantees in conformity with domestic law and consistent with the applicable international obligations of the State Party, including the right to a fair trial and the rights of the defence.

Article 24 also provides for horizontal conditions and safeguards concerning the powers and procedural measures provided by the Convention both at domestic and international levels. It requires States Parties to ensure that, when exercising their procedural powers, those are subject to conditions and safeguards which provide for the protection of human rights, in accordance with their obligations under international human rights law, and which shall incorporate the principle of proportionality. Such conditions and safeguards applicable to the powers and procedures the Convention provides for shall include, among others, judicial or other independent review, the right to an effective remedy (which encompasses several measures for persons whose human rights have been violated), grounds justifying the application, and the limitation of the scope and the duration of the powers and procedures.

Article 36 provides, for the first time in a UN criminal justice instrument, a provision dedicated to the protection of personal data. It applies to any transfer of personal data pursuant to the Convention. Such transfers can only take place in accordance with the domestic law and international law obligations of a transferring State Party. States Parties can refuse to transfer personal data if the data cannot be provided in compliance with their applicable data protection laws, before any personal data can be provided to another State Party. To achieve compliance with its national law on the protection of personal data and be able to respond to a request for international cooperation, a State Party can impose appropriate conditions on the requesting State. States Parties are required to ensure that personal data received by them in accordance with this Convention, either as part of a request for international cooperation or in response to a request, is subject to effective and appropriate safeguards in their respective legal frameworks. States Parties may only transfer the personal data received to a third country or an international organisation with the prior authorization of the original transferring State Party, which may require that the authorization be provided in written form.

The Convention provides for comprehensive safeguards in relation to extradition and mutual legal assistance. States Parties have the ability to refuse extradition or mutual legal assistance requests in the absence of dual criminality, (Article 37 paragraph 1 and Article 40 paragraph 8).

The Convention contains further grounds to refuse cooperation, which are in line with existing international instruments. Article 37 paragraphs 8 and 15, Article 40 paragraphs 8, 21 and 22 enable States Parties to refuse requests for international cooperation in a wide range of cases, for example if a request for mutual legal assistance is not made in conformity with the provisions of Article 40; if the requested State Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests (which is often internationally interpreted to cover also human rights considerations); if the authorities of the requested State Party would be prohibited by its domestic law from carrying out the action requested with regard to any similar offence; if it would be contrary to the legal system of the requested State Party relating to mutual legal assistance; and if the requested State Party has substantial grounds for believing that the request has been made for the purpose of prosecuting or punishing a person on account of that person's sex, race, language, religion, nationality, ethnic origin or political opinions, or that compliance with the request would cause prejudice to that person's position for any one of these reasons. The application of this last safeguard to mutual legal assistance measures, such as the exchange of electronic evidence, is rare in most international instruments on cooperation in criminal matters. It constitutes an important additional guarantee to prevent the targeting of individuals, private sector organisations, media or civil society organisations and their assets. This safeguard, the other grounds for refusal, and the dual criminality requirement enable States Parties to refuse international cooperation on cases that they deem politically motivated.

The human rights conditions and safeguards recognised and provided for in this Convention are part of its object and purpose and inextricably linked to the powers and procedures it provides. As such, these conditions and safeguards cannot be subject to reservations.

The Convention also provides for a periodic review mechanism of the implementation of the Convention by its Conference of States Parties (Article 57 paragraph 5 (f)). This review should cover all the provisions of the Convention, including its conditions and safeguards, in line with other existing international instruments and mechanisms in the same area.

4. BUDGETARY IMPLICATIONS

There are no budgetary implications for the Union budget. EU Member States may have one-off costs for the implementation of the Convention and there could be a moderate increase in costs for authorities of the Member States due to the expected rise in the number of requests for international cooperation.

5. OTHER ELEMENTS

- **Implementation plans and monitoring, evaluation and reporting arrangements**

There is no implementation plan as, following its signature and ratification, Member States will be required to implement the Convention.

With regard to monitoring, the Commission will take part in the meetings of the Conference of the States Parties, where the European Union will be recognised as a Party to the Convention and can exercise voting rights with a number of votes equal to the number of Member States that are Parties to the Convention concerning the adoption of amendments and supplementary protocols to the Convention. The Commission will regularly inform the European Parliament of the outcomes of the review and monitoring of the Convention's implementation conducted by the Conference of States Parties.

- **Detailed explanation of the specific provisions of the proposal**

The aim of the Convention is to enhance international cooperation on criminal offences established in the Convention and the collection of electronic evidence of crimes defined in the Convention and of other serious crimes for the purpose of specific criminal investigations or proceedings. In this regard, the Convention also aims to promote technical assistance and capacity-building, in particular for the benefit of developing countries.

General provisions (*Chapter I (Art. 1-6))*

Chapter I sets out the general scope and purpose of the Convention as well as definitions used therein. For the most part, these provisions are standard formulations and are inspired by the Budapest Convention and the two existing UN criminal justice instruments (UNTOC and UNCAC).

Article 2 provides definitions of terms, which are consistent with those of the Budapest Convention, its Second Additional Protocol and the two existing UN criminal justice instruments (UNTOC and UNCAC). Compared to these instruments there is only one new definition added by the Convention on 'content data' which is inspired by the UNODC Model Law on Mutual Assistance in Criminal Matters[(22)] and by the definition provided in the e-Evidence Regulation.[(23)]

Article 3 determines the scope of application of the Convention as encompassing the prevention, investigation and prosecution of the criminal offences established in accordance with the Convention, as well as the recovery of proceeds of these offences. The scope of the Convention also extends to the collection and sharing of electronic evidence in the framework of specific criminal investigations or proceedings pursuant to Articles 23 and 35 (see further details below under Sections *'Procedural measures and law enforcement (Chapter IV (Art. 23-34))'* and *'International cooperation (Chapter V (Art. 35-52))'*).

Article 4 provides that offences which are established in other applicable UN conventions and protocols (and to which States Parties are a party to), should be punishable irrespective whether that they have been committed offline or online. The second paragraph restricts the scope of this article, by emphasizing that this provision does not provide a legal basis for creating any new or additional offences beyond the ones set out in applicable UN conventions and protocols.

Article 5 is a standard provision on the respect for the principle of sovereignty, replicating the language of the corresponding provisions of UNTOC and UNCAC.

Article 6 is an unprecedented provision compared to the two United Nations criminal justice instruments and the Budapest Convention. It sets out a clear delineation of the object and purpose of the Convention and functions as an important safeguard against its inappropriate use. The first paragraph provides as an overarching high-level objective that all measures taken to implement the Convention must be guided by the international human rights obligations undertaken by each State Party. The second paragraph builds on this objective by reaffirming that the Convention must not be interpreted for the purpose of violating any human rights, whether economic, social and cultural or civil and political rights. This provision includes a non-exhaustive list of rights considered to be particularly susceptible to violations by measures aimed at countering cybercrime such as freedoms of expression,

(22) UNODC Model Law on Mutual Assistance in Criminal Matters (2007), as amended with provisions on electronic evidence and the use of special investigative techniques (2022); E/CN.15/2022/CRP.6.

(23) See Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings Art. 3(12).

conscience, opinion, religion or belief, peaceful assembly and association. Therefore, the scope of the Convention is limited also by this provision, preventing future attempts by States Parties to apply the Convention's international cooperation measures too extensively.

Criminalization (Chapter II (Art. 7-21))

Articles 7-17 set out the harmonisation of the criminalisation of conduct and elements of cyber-dependent and certain cyber-enabled crimes. The cyber-dependent crimes (articles 7-11) are inspired by the crimes set out in the Budapest Convention. The cyber-enabled crimes (articles 12-16) are also inspired by the Budapest Convention and among others, harmonise the offence of information and communication technology system-related fraud (including scams as a type of fraud); the offences related to online child sexual abuse material; as well as the offences of solicitation for the purpose of committing a sexual offence against a child and the non-consensual dissemination of intimate images. All the offences set out in the Convention require two essential elements: intent and that the offence is committed without right. The notion 'without right' is a context-specific requirement for criminal liability that enables States Parties flexibility in application, in accordance with their domestic law and their international obligations. In this regard, the condition 'without right' is meant to ensure that for example conduct of law enforcement authorities when investigating offences or conduct for security, scientific, medical, artistic, or other legitimate, justified or authorised purposes are excluded from the scope of the criminalisation. In this regard, Article 14 paragraph 4 provides for an explicit exemption from criminalisation of conduct by children for self-generated material depicting them or the consensual production, transmission, or possession of material described in paragraph 2 (a) to (c) of Article 14, where the underlying conduct depicted is legal as determined by domestic law, and where such material is maintained exclusively for the private and consensual use of the persons involved.

Article 17 requires the criminalisation of laundering the proceeds of crimes and is inspired by corresponding provisions in UNTOC and UNCAC. According to the Interpretative notes on specific articles of the Convention, which are annexed to the resolution adopting the Convention, a conduct shall only be deemed an offence under Article 17 when the underlying criminal conduct associated with the more complex crime of laundering of the proceeds is an offence established in accordance with articles 7 to 16 of the Convention.

Article 18 replicates the corresponding provisions of UNTOC and UNCAC on establishing minimum rules on the liability of legal persons for the offences set out in accordance with this Convention (i.e. offences set out in Articles 7-17). Such liability is attached to legal persons' participation in one of the criminal offences codified in Articles 7-17, subject to the same requirements applicable to natural persons of committing them 'intentionally and without right', and to each State Party's legal principles (paragraphs 1 and 2).

Articles 19 and 20 echo the corresponding provisions of UNTOC and UNCAC by providing for minimum rules on establishing the offences of participation, attempt and preparation and statute of limitation periods in accordance with States Parties' domestic laws and as necessary for offences set out in the Convention. Although the online transmission and controlling of data that might be relevant for an offence rely on the assistance of service providers, a service provider that does not have the criminal intent is not meant to incur liability under Article 19. Thus, there shall be no duty on a service provider to actively monitor content to avoid criminal liability under this provision.

Article 21 is also inspired by UNTOC and UNCAC, it provides for minimum rules on the prosecution, adjudication and sanctions concerning the offences established in accordance with the Convention. Paragraph 4 requires States Parties to ensure that any person prosecuted for offences established in accordance with the Convention enjoys all rights and guarantees

consistent with the international obligations of the States Parties, including the right to a fair trial and the rights of the defence.

Jurisdiction (Chapter III (Art. 22))

Article 22 also reflects the corresponding provisions of UNTOC, UNCAC and the Budapest Convention, and it regulates the establishment of mandatory and optional forms of jurisdiction as necessary over the offences established in accordance with the Convention.

Procedural measures and law enforcement (Chapter IV (Art. 23-34))

Article 23 determines the scope of domestic powers and procedural measures that enable international cooperation: it applies to specific criminal investigations or proceedings concerning criminal offences established in accordance with the Convention; other criminal offences committed by means of an information and communications technology system as well as to the collection of evidence in electronic form of any criminal offence. According to the Interpretative notes on specific articles of the Convention which is annexed to the resolution adopting the Convention: 'The term "criminal investigations" covers situations where there are reasonable grounds to believe, on the basis of factual circumstances, that a criminal offence (including an offence set out in Article 19 of the Convention) has been committed or is being committed, including when such an investigation is aimed at stopping or impeding the commission of the offence in question.' Thus, the Convention does not provide a basis for international cooperation regarding preventative purposes and data can only be exchanged if it relates to a specific criminal investigation.

Article 24 reproduces, with a few changes, the corresponding language of Article 15 of the Budapest Convention. It provides for over-arching conditions and safeguards to ensure that the powers and procedures set out in Chapter IV are subject to an appropriate level of protection for fundamental rights, including the application of the principle of proportionality. Such conditions and safeguards shall include, inter alia, judicial or other independent review, the right to an effective remedy, grounds justifying application, and limitation of the scope and the duration of such power or procedure. Furthermore, the conditions and safeguards established in accordance with this article shall apply at the domestic level to the powers and procedures set forth in Chapter IV, both for the purpose of domestic criminal investigations and proceedings and for the purpose of rendering international cooperation by the requested State Party pursuant to Chapter V.

Articles 25-30 are inspired by the corresponding domestic powers and procedural measures of the Budapest Convention. These are: expedited preservation of stored electronic data; expedited preservation and partial disclosure of traffic data; production order; search and seizure of stored electronic data; real-time collection of traffic data and interception of content data.

Article 31 reflects Article 31 of UNCAC. It requires States Parties to adopt measures to enable the freezing, seizure and confiscation of the proceeds of crime.

Article 32 is inspired by UNTOC and UNCAC and provides the possibility for States Parties to establish criminal records for the purpose of using such information in criminal proceedings relating to an offence established in accordance with the Convention.

Article 33 is inspired by UNTOC and requires States Parties to take appropriate measures in accordance with their domestic laws, to provide adequate protection to witnesses.

Article 34 is inspired by UNTOC and require States Parties, in accordance with their domestic laws, to take appropriate measures to provide adequate assistance to victims, particularly to victims of offences established in articles 14-16 of the Convention. When applying its

paragraphs 2-4, Article 34 also requires States Parties to take into account the age, gender and the particular circumstances and needs of victims, including the particular circumstances and needs of children. Paragraph 6 encourages States Parties to take effective steps to ensure compliance with requests to remove or render inaccessible the content described in articles 14 and 16 of this Convention to the extent consistent with their domestic legal frameworks.

International cooperation (Chapter V (Art. 35-52))

Article 35 sets out the general principles and scope of international cooperation which requires States Parties to cooperate with each other for the purpose of investigating and prosecuting and the collecting and sharing of electronic evidence of criminal offences established in accordance with the Convention as well as the collecting and sharing of electronic evidence of any serious crime punishable by a maximum deprivation of liberty of at least four years or a more serious penalty. Therefore, the scope of international cooperation is limited to crimes established in accordance with the Convention and serious crimes with a clear penalty threshold.

Article 36 provides an explicit provision on the protection of personal data. This provision regulates the rules for transferring personal data in the framework of international cooperation. Transfer can only take place in accordance with the domestic law and international law obligations of a transferring States Party. States Parties can refuse to transfer personal data if the data cannot be provided in compliance with their applicable laws concerning the protection of personal data. For the EU, this means that important data protection principles, including purpose limitation, data minimisation, proportionality and necessity must be applied, in accordance with the Charter of Fundamental Rights of the European Union, before any personal data can be provided to another State Party. States Parties can also seek to impose appropriate conditions to achieve compliance in order to respond to a request for personal data. States Parties are required to ensure that personal data received by them in accordance with this Convention is subject to effective and appropriate safeguards in their respective legal frameworks. States Parties may only transfer the personal data received to a third country or an international organisation with the prior authorization of the original transferring State Party, which may require that the authorization be provided in written form.

Article 37 is inspired by UNCAC and the Budapest Convention and provides detailed rules on extradition. Pursuant to paragraph 8, the Convention allows for refusal of extradition based on conditions set out in the requested State Party's national law. Paragraph 15 establishes a further ground to refuse a request for extradition if it has been made for the purpose of prosecuting or punishing a person on account of that person's sex, race, language, religion, nationality, ethnic origin or political opinions, or that compliance with the request would cause prejudice to that person's position for any one of these reasons.

Articles 38 and 39 are inspired by UNTOC and UNCAC and establish the possibility for transferring sentenced persons and criminal proceedings.

Article 40 echoes provisions of UNTOC, UNCAC and the Budapest Convention and sets out detailed provisions on the principles and procedures relating to mutual legal assistance. Paragraph 17 requires requests for mutual legal assistance to be executed in accordance with the domestic law of the requested State Party. Paragraph 19 prohibits a requesting State Party from transmitting or using information or evidence furnished by the requested State Party for investigations, prosecutions or judicial proceedings other than those stated in the request without the prior consent of the requested State Party. Paragraphs 8, 21 and 22 provide for comprehensive grounds to refuse requests for mutual legal assistance as described in the Section on *'Fundamental rights'*.

Article 41 is inspired by Article 35 of the Budapest Convention and requires State Parties to set up 24/7 networks to provide assistance for specific investigations prosecutions or judicial proceedings concerning offences established in accordance with the Convention or the collection of electronic evidence.

Articles 42-46 echo Articles 29-33 of the Budapest Convention and set out the details of specific types of international cooperation measures for mutual legal assistance. Such measures are: expedited preservation of stored electronic data; expedited disclosure of preserved traffic data; accessing stored electronic data; real-time collection of traffic data and interception of content data. With regard to the most intrusive measures of real-time collection of traffic data and interception of content data, States Parties have a more limited obligation to "endeavour" to provide such assistance. This obligation constitutes in essence a 'best-efforts obligation' and is thus less constraining on States Parties than the obligations for other mutual legal assistance measures, which require cooperating with other States Parties unless the applicable conditions are not met or one of the applicable grounds for refusal is exercised. Furthermore, assistance for interception of content data can only be requested for serious criminal offences to the extent permitted under treaties applicable to States Parties or under their domestic laws.

Articles 47 and 48 are inspired by UNTOC and UNCAC and encourages States Parties to cooperate to enhance the law enforcement action to combat offences established in accordance with the Convention and to establish joint investigative bodies for the same purpose.

Articles 49-52 are inspired by UNTOC and/or UNCAC and provide minimum rules on measures for the confiscation, recovery and return of proceeds or property of the crimes established in accordance with the Convention.

Preventive measures (Chapter VI (Art. 53))

Article 53 encourages States Parties to endeavour, in accordance with fundamental principles of their legal systems, to develop and implement or maintain effective and coordinated policies and best practices to reduce existing or future opportunities for cybercrime through appropriate legislative, administrative or other measures. States Parties should promote the active participation of relevant individuals and entities outside the public sector, such as non-governmental organizations, civil society organizations, academic institutions and private sector entities, as well as the general public, in the relevant aspects of prevention of the offences established in accordance with the Convention. Paragraph 3 provides a non-exhaustive and non-binding list of preventive measures. Subparagraph (e) of paragraph 3 provides an explicit reference to preventive measures recognizing the contributions of the legitimate activities of security researchers when intended solely to strengthen and improve the security of service providers' products, services and customers.

Technical assistance and information exchange (Chapter VII (Art. 54-56))

Articles 54-56 are inspired by UNTOC and/or UNCAC and set out provisions on providing technical assistance, capacity building and exchange of information taking into particular consideration the interests and needs of developing States Parties.

Mechanism of implementation (Chapter VIII (Art. 57-58))

Articles 57 and 58 are inspired by UNCAC and set out details on the Conference of the States Parties which will oversee the implementation of the Convention and will have the competence to elaborate and adopt supplementary protocols to the Convention on the basis of Articles 61 and 62 of the Convention. The Secretary-General of the United Nations shall provide the secretary services and convene the Conference of the States Parties not later

than one year following the entry into force of the Convention. Thereafter, regular meetings of the Conference shall be held in accordance with the rules of procedure adopted by the Conference.

Final provisions (Chapter IX (Art. 59-68))

Chapter IX of the Convention contains the final provisions. Amongst others, Article 60 paragraph 1 ensures that EU Member States that are Party to the Convention can continue to apply Union law in their mutual relations. It also allows the Parties to the Budapest Convention and to other international instruments to continue applying those instruments between themselves.

Article 64 paragraph 1 provides that the Convention shall be open to all States for signature in Hanoi in October 2025 and thereafter at United Nations Headquarters in New York until 31 December 2026. According to paragraph 2, the Convention shall also be open for signature by regional economic integration organizations such as the Union, provided that at least one Member State has signed the Convention in accordance with paragraph 1.

Article 64 paragraph 3 and Article 65 paragraph 1 indicate that the Convention shall enter into force once forty States have expressed their consent to be bound by the Convention by depositing their instruments of ratification, acceptance or approval with the Secretary-General of the United Nations. Regional economic integration organizations such as the Union may deposit their instrument of ratification, acceptance or approval if at least one of their Member States has done likewise. In that instrument of ratification, acceptance or approval, a regional economic integration organization shall declare the extent of its competence with respect to the matters governed by this Convention. According to Article 64 paragraph 4, the Convention is open for accession by regional economic integration organizations such as the Union on the condition that least one Member State is a Party to the Convention. At the time of its accession, the Union shall declare the extent of its competence with respect to matters governed by the Convention.

According to Article 66 paragraph 1, five years from the entry into force of the Convention, a State Party may propose an amendment and transmit it to the Secretary-General of the United Nations, who shall thereupon communicate the proposed amendment to the States Parties and to the Conference of the States Parties to the Convention for the purpose of considering and deciding on the proposal. Based on paragraph 2, regional economic integration organizations such as the Union, in matters within its competence, shall exercise their right to vote with a number of votes equal to the number of its Member States that are Parties to the Convention. An amendment adopted in accordance with paragraph 1 is subject to ratification, acceptance or approval by States Parties.

Articles 61 and 62 provide rules on protocols supplementary to the Convention. Article 61 paragraph 2 allows regional economic integration organizations such as the Union to become a Party to a protocol only if the organisation is a Party to the Convention. According to paragraph 4, any protocol to the Convention shall be interpreted together with the Convention, taking into account the purpose of that protocol. Article 62 paragraph 1 requires at least sixty States Parties before any supplementary protocol is considered for adoption by the Conference of the States Parties. That article also provides that the Conference of the States Parties shall make every effort to achieve consensus on any supplementary protocol, and only when all efforts have been exhausted, it shall as a last resort require for its adoption at least a two-thirds majority vote of the States Parties present and voting at the meeting of the Conference of the States Parties. According to paragraph 2 of Article 62, regional economic integration organizations such as the Union, in matters within its competence, shall exercise

their right to vote under this article with a number of votes equal to the number of their Member States that are Parties to the Convention.

Based on Article 67 paragraph 2, regional economic integration organizations such as the Union shall cease to be a Party to the Convention when all of their Member States have denounced it.

The resolution adopting the Convention is accompanied by interpretative notes on articles 2, 17, 23 and 35. Although such interpretative notes do not constitute an instrument providing an authoritative interpretation of the Convention, they are intended to guide and assist Parties in its application. The UN AHC's Chair's interpretative notes distributed during the negotiations also address several key aspects of interpretation. The website of the Ad Hoc Committee includes all proposals and revisions of the draft text of the Convention during the negotiations and thus provides useful information on the development of key provisions within the text and can have interpretative value. Furthermore, the Explanatory Report to the Budapest Convention[(24)] can also serve as a helpful, even if informal, infomration tool for States for many provisions that were inspired by the Budapest Convention, such as most of the Convention's criminalisation and procedural powers provisions.

(24) European Treaty Series - No. 185

2025/0231 (NLE)

Proposal for a

COUNCIL DECISION

on the conclusion, on behalf of the European Union, of the United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 16, 82(1), 83(1) and 87(2) in conjunction with Article 218(6) thereof,

Having regard to the proposal from the European Commission,

Having regard to the consent of the European Parliament,

Whereas:

(1) In accordance with Council Decision (EU) [signing decision], the United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes (the 'Convention') was signed on [date], on behalf of the Union, subject to its conclusion at a later date.

(2) The Convention is in conformity with the security objectives of the European Union as referred to in Article 67(3) of the Treaty on the Functioning of the European Union, namely ensuring a high level of security through measures to prevent and combat crime and through measures for coordination and cooperation between police and judicial authorities and other competent authorities, as well as through the approximation of criminal laws.

(3) The provisions of the Convention apply to specific criminal investigations or proceedings concerning criminal offences established in accordance with the Convention and only allow for data exchange for such a purpose.

(4) The Convention harmonizes a limited set of clearly defined offences while allowing the necessary flexibility for State Parties to avoid overcriminalization of legitimate conduct.

(5) The Convention establishes only minimum rules on the liability of legal persons for the offences set out therein and does not require establishing such criminal liability in a manner that would be inconsistent with a State Party's legal principles.

(6) The Convention is also in conformity with the personal data, privacy and fundamental rights protection objectives of the European Union in line with Article 16 of the Treaty on the Functioning of the European Union and the Charter of Fundamental Rights of the European Union.

(7) The Convention provides for robust human rights safeguards and excludes any interpretation that would lead to suppressing human rights or fundamental freedoms, in particular the freedoms of expression, conscience, opinion, religion or belief, peaceful assembly and

association. These safeguards also ensure that international cooperation can be refused if such cooperation would be contrary to States Parties' domestic laws or would be necessary to avoid any form of discrimination.

(8) Concerning the powers and procedural measures both at domestic and international levels, the Convention provides for horizontal conditions and safeguards ensuring the protection of human rights, in accordance with State Parties' obligations under international human rights law, and which shall incorporate the principle of proportionality. Such conditions and safeguards shall include, among others, judicial or other independent review, the right to an effective remedy, grounds justifying application and the limitation of the scope and the duration of the powers and procedures.

(9) The Convention includes a dedicated provision on the protection of personal data which ensures that important data protection principles, including purpose limitation, data minimisation, proportionality and necessity must be applied, in accordance with the Charter of Fundamental Rights of the European Union, before any personal data can be provided to another State Party.

(10) With its participation in the negotiations, on behalf of the Union, the Commission ensured compatibility of the Convention with relevant European Union rules.

(11) A number of reservations and notifications are relevant to ensure compatibility of the Convention with Union law and policies, as well as the uniform application of the Convention amongst EU Member States in their relations with non-EU State Parties, and the effective application of the Convention.

(12) The reservations and notifications, on which guidance is given in Annex I to this Decision, are without prejudice to any other reservations or declarations that Member States might wish to make individually where permissible.

(13) Given that the Convention provides for procedures that improve cross-border access to electronic evidence and a high level of safeguards, becoming a Party to it will promote consistency in the European Union's efforts in combating cybercrime and other forms of crime at global level. It will facilitate cooperation between the EU Member State Parties and the non-EU Member State Parties to the Convention while ensuring a high level of protection of individuals.

(14) Becoming a Party to the Convention by the European Union will furthermore ensure that the Union has a meaningful voice early in the implementation of this new global framework for the fight against cybercrime.

(15) Pursuant to its Article 64(3), the Convention is subject to ratification, approval or acceptance by States and regional economic integration organisations, such as the Union.

(16) The conclusion of the Convention by the Union is without prejudice to the Member States' competence as regards the ratification, approval or acceptance of the Convention.

(17) In accordance with Article 64(3) and (4) of the Convention, the Union should, in its instrument of ratification, acceptance, approval or accession declare the extent of its competence in respect of the matters governed by the Convention ('Declaration of Competence' – Annex II).

(18) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council and delivered an opinion on [...].

(19) [In accordance with Article 3 of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and the Treaty on the Functioning of the European Union, Ireland has notified [, *by letter of* …,] its wish to take part in the adoption and application of this Decision."] OR

[In accordance with Articles 1 and 2 of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, and without prejudice to Article 4 of that Protocol, Ireland is not taking part in the adoption of this Decision and is not bound by it or subject to its application.]

(20) In accordance with Articles 1 and 2 of Protocol No 22 on the position of the Kingdom of Denmark, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, the Kingdom of Denmark is not taking part in the adoption of this Decision and is not bound by it or subject to its application.

(21) The Convention, the attached reservations and notifications, and the Declaration of Competence should be approved,

HAS ADOPTED THIS DECISION:

Article 1

The United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes (the 'Convention') is hereby approved on behalf of the European Union.

The text of the Convention is attached to this Decision (Annex III).

Article 2

The Declaration of Competence required by Article 64(3) and (4) of the Convention is hereby approved.

The Declaration of Competence is attached to this Decision (Annex II).

Article 3

The reservations and notifications set out in Annex I are hereby approved.

Article 4

This Decision shall enter into force on the date following that of its adoption.

Done at Brussels,

For the Council
The President