Basic information

2021/0383(NLE) NLE - Non-legislative enactments	Awaiting final decision
Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence: Second Additional Protocol **Subject** 3.30.07 Cybersecurity, cyberspace policy 3.30.25 International information networks and society, internet	

Key players

European Parliament	**Committee responsible**	**Rapporteur**	**Appointed**
	LIBE Civil Liberties, Justice and Home Affairs	LÓPEZ AGUILAR Juan Fernando (S&D)	05/09/2019
		Shadow rapporteur MELO Nuno (EPP) KÖRNER Moritz (Renew) LAGODINSKY Sergey (Greens/EFA) KANKO Assita (ECR) TARDINO Annalisa (ID)	
Council of the European Union			
European Commission	**Commission DG**	**Commissioner**	
	Migration and Home Affairs	JOHANSSON Ylva	

Key events

Date	Event	Reference	Summary
25/11/2021	Preparatory document	COM(2021)0719	
06/04/2022	Legislative proposal published	06438/2022	Summary
07/04/2022	Committee referral announced in Parliament		
12/01/2023	Vote in committee		
13/01/2023	Committee report tabled for plenary, 1st reading/single reading	A9-0002/2023	
17/01/2023	Decision by Parliament	T9-0002/2023	Summary

17/01/2023	Results of vote in Parliament		

Technical information

Procedure reference	2021/0383(NLE)
Procedure type	NLE - Non-legislative enactments
Procedure subtype	Consent by Parliament
Stage reached in procedure	Awaiting final decision
Committee dossier	LIBE/9/07837

Documentation gateway

European Parliament

Document type	Committee	Reference	Date	Summary
Committee draft report		PE740.540	21/12/2022	
Amendments tabled in committee		PE740.618	10/01/2023	
Committee report tabled for plenary, 1st reading/single reading		A9-0002/2023	13/01/2023	
Text adopted by Parliament, 1st reading/single reading		T9-0002/2023	17/01/2023	Summary

Council of the EU

Document type	Reference	Date	Summary
Legislative proposal	06438/2022	06/04/2022	Summary

European Commission

Document type	Reference	Date	Summary
Document attached to the procedure	COM(2021)0718	25/11/2021	
Preparatory document	COM(2021)0719	25/11/2021	Summary

Other institutions and bodies

Institution/body	Document type	Reference	Date	Summary
EDPS	Document attached to the procedure	N9-0021/2022 OJ C 182 04.05.2022, p. 0015	20/01/2022	

Additional information

Source	Document	Date

European Commission	EUR-Lex	

Meetings with interest representatives published in line with the Rules of Procedure

Other Members

Transparency		
Name	Date	Interest representatives
SIPPEL Birgit	11/01/2023	Council of Europe

Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence: Second Additional Protocol

2021/0383(NLE) - 17/01/2023 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted, by 436 votes to 168, with 35 abstentions, a legislative resolution on the draft Council decision 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.

Following the recommendation of the Committee on Civil Liberties, Justice and Home Affairs, Parliament gave its consent to the Council's draft decision.

The draft Council decision aims to authorise Member States to ratify, in the interest of the EU, the second additional protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence.

The objective of the protocol is to strengthen cooperation on cybercrime and the collection of electronic evidence of a criminal offense for the purpose of specific investigations or criminal proceedings. The protocol recognises the need for increased and more efficient cooperation between States and the private sector, and greater clarity or legal certainty for service providers and other entities regarding the circumstances under which they may respond to requests from criminal justice authorities in other Parties for the disclosure of electronic evidence.

The protocol also recognises that effective conditions and guarantees in terms of protecting fundamental rights are essential for effective cross-border cooperation for criminal justice, including between the public and private sectors. To this end, the protocol follows a rights-based approach and provides for conditions and guarantees that conform to international human rights instruments, including the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms.

The protocol also provides for strong safeguards for the protection of privacy and personal data.

Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence: Second Additional Protocol

2021/0383(NLE) - 25/11/2021

PURPOSE: to authorise 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.

PROPOSED ACT: Council Decision.

ROLE OF THE EUROPEAN PARLIAMENT: Council may adopt the act only if Parliament has given its consent to the act.

BACKGROUND: cybercrime continues to represent a considerable challenge to society. Notwithstanding the efforts of law enforcement and judicial authorities, cyberattacks, including ransomware attacks, are increasing and are becoming more complex. The borderless nature of the internet makes cybercrime investigations almost always cross-border in nature, thus requiring close cooperation between authorities in different countries.

The Commission estimates that **law enforcement and judicial authorities currently need access to electronic evidence in 85% of criminal investigations**, including cybercrime. As evidence of criminal offences is increasingly held in electronic form by service providers on the territory of foreign jurisdictions, the Commission considers it necessary to obtain such evidence by appropriate measures to uphold the rule of law.

The Council of Europe's **Budapest Convention on Cybercrime** aims to facilitate the fight against criminal offences committed through computer networks. 66 countries are currently party to the Convention, including 26 EU Member States. The Convention does not provide for the European

Union to accede to the Convention. However, the EU supports the Budapest Convention, which remains the main multilateral convention for combating cybercrime.

On 9 June 2019, the Council authorised the Commission to participate, on behalf of the Union, in the negotiations for the **Second Additional Protocol** to the Council of Europe Budapest Convention on Cybercrime. The text of the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence was adopted by the Council of Europe Committee of Ministers on 17 November 2021 and is envisaged to be opened for signature in March 2022.

It is important that EU Member States take the necessary steps to **implement and ratify rapidly the Protocol**, as the Protocol:

- will ensure that law enforcement and judicial authorities are better equipped to obtain electronic evidence necessary for criminal investigations;

- will ensure that such measures to obtain access to electronic evidence will be used in a manner that allow Member States to respect fundamental rights, including criminal procedural rights, the right to privacy and the right to the protection of personal data;

- will resolve and prevent conflicts of law, affecting both authorities and private sector service providers and other entities, by providing compatible rules at international level for cross-border access to electronic evidence.

CONTENT: this proposal concerns the Decision authorising Member States to ratify, in the interest of the European Union, the Second Additional Protocol to the Council of Europe's Budapest Convention on Cybercrime, on enhanced co-operation and disclosure of electronic evidence.

The purpose of the Protocol is to establish common rules at international level to **enhance cooperation in relation to cybercrime and the gathering of evidence in electronic form** for criminal investigations or proceedings.

The Protocol recognises the need for **greater cooperation between States and the private sector** and for greater legal certainty for service providers and other entities regarding the circumstances in which they may respond to requests for disclosure of electronic evidence from criminal justice authorities in other parties.

The Protocol provides a basis:

- for the direct cooperation between competent authorities in one Party and entities providing domain name registration services in another Party, for the disclosure of domain name registration data;

- for the direct cooperation between competent authorities in one Party and service providers in another Party for the disclosure of subscriber data;

- for enhanced cooperation between authorities for the disclosure of computer data and cooperation between authorities for the disclosure of computer data in emergency situations;

- for mutual legal assistance in emergency situations, cooperation by videoconference and for joint investigations and joint investigation teams.

The Protocol requires the parties to ensure that powers and procedures are subject to an adequate level of protection of fundamental rights.

Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence: Second Additional Protocol

2021/0383(NLE) - 06/04/2022 - Legislative proposal

PURPOSE: to authorise Member States to ratify, 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.

PROPOSED ACT: Council Decision.

ROLE OF THE EUROPEAN PARLIAMENT: Council may adopt the act only if Parliament has given its consent to the act.

BACKGROUND: cybercrime continues to represent a considerable challenge to our society. The borderless nature of the internet makes cybercrime investigations almost always cross-border in nature, thus requiring close cooperation between authorities in different countries.

As evidence of criminal offences is increasingly held in electronic form by service providers in the territory of foreign jurisdictions, and to enable an effective criminal justice response, it is necessary to obtain such evidence by appropriate measures in order to uphold the rule of law.

On 6 June 2019, the Council authorised the Commission to participate, on behalf of the Union, in the negotiations on a Second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185) (the Convention on Cybercrime).

The Budapest Convention on Cybercrime aims to facilitate the fight against criminal offences committed through computer networks. The Convention:

- contains provisions harmonising domestic criminal substantive law elements of offences and connected provisions in the area of cybercrime;

- provides for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or where the evidence is in electronic form;

- aims to set up a fast and effective regime of international cooperation.

The Commission is committed to ensuring a swift conclusion of the negotiations on the Protocol. In participating in the negotiations on the Protocol, the Commission has ensured its compatibility with the relevant common rules of the Union. The European Parliament also recognised the need to conclude work on the Protocol in its 2021 resolution on the EU cybersecurity strategy for the digital decade.

The Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence was adopted by the Committee of Ministers of the Council of Europe on 17 November 2021 and is envisaged to be opened for signature on 12 May 2022.

The provisions of the Protocol fall within an area covered to a large extent by common rules within the meaning of Article 3(2) of the Treaty on the Functioning of the European Union (TFEU), including instruments facilitating judicial cooperation in criminal matters, ensuring minimum standards of procedural rights as well as data protection and privacy safeguards.

CONTENT: the purpose of the draft Council Decision is to authorise Member States to ratify, in the interest of the European Union, the **Second Additional Protocol to the Convention on Cybercrime**, on enhancing cooperation and the provision of electronic evidence.

The aim of the Protocol is to **enhance co-operation on cybercrime** and the collection of evidence in electronic form of a criminal offence for the purpose of specific criminal investigations or proceedings.

The Protocol recognises the need for increased and more efficient co-operation between States and with the private sector, and for greater clarity and legal certainty for service providers and other entities regarding the circumstances in which they may respond to requests from criminal justice authorities in other Parties for the **disclosure of electronic evidence**.

The Protocol also recognises that effective cross-border cooperation for criminal justice purposes, including between public sector authorities and private sector entities, requires effective conditions and strong safeguards for the protection of fundamental rights.

The Protocol:

- applies to specific criminal investigations or proceedings concerning criminal offences related to computer data and systems and to the collection of evidence in electronic form of a criminal offence;

- determines the languages in which the parties must submit orders, requests or notifications under the Protocol;

- provides for the widest possible mutual cooperation between the parties and provides for **swift procedures that improve cross-border access to electronic evidence** and a high level of safeguards. Its entry into force will contribute to the fight against cybercrime by facilitating cooperation between Member States party to the Protocol and third countries party to the Protocol, ensure a high level of protection for individuals and resolve conflicts of law.

The Protocol provides a basis for:

- direct co-operation between the competent authorities in the territory of one Party and entities providing domain name registration services in the territory of another Party, for the disclosure of domain name registration data;

- direct cooperation between the competent authorities in the territory of a Party and service providers in the territory of another Party, for the disclosure of subscriber data;

- enhanced cooperation between authorities for the disclosure of computer data;

- cooperation between authorities for the disclosure of computer data in emergency situations;

- mutual legal assistance in emergency cases;

- cooperation by videoconference;

- joint investigations and joint investigation teams.

The entry into force of the Protocol will help promote EU data protection standards at global level, facilitate data flows between Member State Parties and third-country Parties, and ensure compliance of Member State Parties with their obligations under Union data protection rules.

Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence: Second Additional Protocol

2021/0383(NLE) - 06/04/2022

PURPOSE: to authorise Member States to ratify, 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.

PROPOSED ACT: Council Decision.

ROLE OF THE EUROPEAN PARLIAMENT: Council may adopt the act only if Parliament has given its consent to the act.

BACKGROUND: cybercrime continues to represent a considerable challenge to our society. The borderless nature of the internet makes cybercrime investigations almost always cross-border in nature, thus requiring close cooperation between authorities in different countries.

As evidence of criminal offences is increasingly held in electronic form by service providers in the territory of foreign jurisdictions, and to enable an effective criminal justice response, it is necessary to obtain such evidence by appropriate measures to uphold the rule of law.

On 6 June 2019, the Council authorised the Commission to participate, on behalf of the Union, in the negotiations on a Second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185) (the Convention on Cybercrime).

The Budapest Convention on Cybercrime aims to facilitate the fight against criminal offences committed through computer networks. The Convention:

- contains provisions harmonising domestic criminal substantive law elements of offences and connected provisions in the area of cybercrime;

- provides for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or where the evidence is in electronic form;

- aims to set up a fast and effective regime of international cooperation.

The Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence was adopted by the Committee of Ministers of the Council of Europe on 17 November 2021 and is envisaged to be opened for signature on 12 May 2022.

The provisions of the Protocol fall within an area covered to a large extent by common rules within the meaning of Article 3(2) of the Treaty on the Functioning of the European Union (TFEU), including instruments facilitating judicial cooperation in criminal matters, ensuring minimum standards of procedural rights as well as data protection and privacy safeguards.

The Commission also presented a proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters and a proposal for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, which introduce binding cross-border European production and preservation orders to be issued directly to a representative of a service provider in another Member State.

In participating in the negotiations on the Protocol, the Commission has ensured its compatibility with the relevant common EU rules.

CONTENT: the purpose of the draft Council Decision is to authorise Member States to ratify, 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.

The objective of the Protocol is to **strengthen cooperation on cybercrime and the gathering of evidence in electronic form of a criminal offence** for the purpose of specific criminal investigations or proceedings.

The Protocol provides for swift procedures that improve cross-border access to electronic evidence and a high level of safeguards. Therefore, its entry into force will contribute to the fight against cybercrime and other forms of crime at global level by facilitating cooperation between the EU Member State Parties and the non-EU Member State Parties to the Protocol, will ensure a high level of protection of individuals, and will address conflicts of law.

The Protocol provides for appropriate safeguards in line with the requirements for international transfers of personal data under Regulation (EU) 2016 /679 and Directive (EU) 2016/680. Therefore, its entry into force will contribute to the promotion of Union data protection standards at global level, facilitate data flows between the EU Member State Parties and the non-EU Member State Parties to the Protocol, and will ensure compliance of EU Member States with their obligations under Union data protection rules.

The Protocol provides a basis for:

- direct co-operation between the competent authorities in the territory of one Party and entities providing domain name registration services in the territory of another Party, for the disclosure of domain name registration data;

- direct cooperation between the competent authorities in the territory of a Party and service providers in the territory of another Party, for the disclosure of subscriber data;

- enhanced cooperation between authorities for the disclosure of computer data;

- cooperation between authorities for the disclosure of computer data in emergency situations;

- mutual legal assistance in emergency cases;

- cooperation by videoconference;

- joint investigations and joint investigation teams.