CyberSPEX

Enhanced co-operation on e-evidence by EU Member States through the Second Protocol to the Budapest Convention

Project outline

CyberSPEX: Enhanced co-operation on e-evidence by EU Member States through the Second Protocol to the Budapest Convention

Version 24 January 2024

Project title / number:	CyberSPEX: Enhanced co-operation on e-evidence by EU Member States through the Second Protocol to the Budapest Convention on Cybercrime
Project area:	European Union Member States (3798)
Duration:	24 months (1 March 2024 – 28 February 2026) [TBC]
Budget:	EURO 2.23 million
Funding:	European Union (90%)/Council of Europe (10%)
Implementation:	Cybercrime Programme Office (C-PROC) of the Council of Europe

BACKGROUND AND JUSTIFICATION

The Budapest Convention on Cybercrime serves as a global framework for cooperation on cybercrime and electronic evidence. By December 2023, 69 States were Parties and another 22 had signed it or been invited to accede. Parties include all EU Member States (m/s) except Ireland which had signed it in 2002.

In May 2022, the Second Additional Protocol to the Budapest Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence was opened for signature. By December 2023, two States (Japan and Serbia) were Parties, and a further 41 States had signed it, including 20 EU m/s. The project will encourage signature by all EU m/s. It will also support EU m/s to permit them to ratify this Protocol as soon as possible.

The Second Protocol responds to challenges and complexities of obtaining electronic evidence that may be stored in foreign, multiple, shifting or unknown jurisdictions. It does so by providing tools for enhanced co-operation and disclosure of electronic evidence that are subject to a system of human rights and rule of law, including data protection safeguards:

- Article 4 Language
- Article 6 Request for domain name registration information
- Article 7 Disclosure of subscriber information
- Article 8 Giving effect to orders from another party for expedited production of subscriber information and traffic data

Co-funded by the European Union
EUROPEAN UNION
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
Co-funded and implemented by the Council of Europe

- Article 9 Expedited disclosure of stored computer data in an emergency
- Article 10 Emergency mutual assistance
- Article 11 Video conferencing
- Article 12 Joint investigation teams and joint investigations
- Article 13 Conditions and safeguards
- Article 14 Protection of personal data

The project will support EU m/s in the development of the relevant domestic legislation and of other measures to operationalise the provisions of the Protocol.

In May 2022, EU Council Decision 2022/722 authorised EU m/s to sign the Second Protocol. In February 2023, EU Council Decision 2023/436 also authorised them to ratify it. According to this decision, EU m/s are required to make a number of declarations and reservations when becoming Parties to this Protocol. For example, EU m/s will be required to invoke the notification mechanism of Article 7.5 with respect to direct cooperation with service providers in other Parties for the production of subscriber information. They will also be required to declare a number of authorities.[1] The project will support EU m/s in the implementation of these requirements.

In August 2023, the European Union's Regulation EU 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence entered into force. It is complemented by Directive EU 2023/1544 on rules for designated establishments and legal representatives for the gathering of electronic evidence. The Regulation will become applicable as of 17 August 2026 and the Directive as of 17 February 2026.

The interaction of the Second Protocol with other instruments, including the E-evidence Regulation and Directive, raises a number of questions that the project will help clarify. As EU m/s will cooperate with each other primarily on the basis of EU law, the Second Protocol will assist EU m/s in particular in their cooperation with non-EU countries. The project will therefore focus on the practical procedures for their cooperation with third countries that are Parties to the Convention and are signatories or Parties to the Second Protocol.

METHODOLOGY AND ARRANGEMENTS FOR IMPLEMENTATION

The project will be implemented by the Council of Europe's Cybercrime Programme Office (C-PROC) in Bucharest. C-PROC is part of the Cybercrime Division which also includes the Secretariat of the Cybercrime Convention Committee (T-CY) that represents the Parties to the Budapest Convention. This arrangement permits to make full use not only of the experience of C-PROC in capacity building but also the expertise of the T-CY that had negotiated the Second Protocol.

The C-PROC online training platform will be used for capacity building activities and online resources.

The project will seek close cooperation with organisations with subject-matter expertise on cybercrime and e-evidence, that is, EUROJUST and EUROPOL, including the SIRIUS project, as well as CEPOL.

In order to achieve maximum progress within the timeframe of the project, four to six pilot countries will be selected from among those m/s that have signed the Second Protocol. A more detailed set of

[1] Article 6.6, Article 7.5.e, Article 8.10, and Articles 14.7.c and 14.10.b. With regard to Article 10.5 related to emergency mutual assistance, the project will also facilitate the preparation of a directory of relevant authorities (see paragraph 177 of the Explanatory Report to the Protocol) and the compilation of information on policies of entities and providers as detailed in paragraphs 84.d, 106 and 165 of the Explanatory Report.

activities, including in-country activities, will be supported in these m/s. Lessons learnt from and procedures or templates developed with these pilot countries will then be shared with all EU m/s.

In order to further support the sharing of experience across m/s, each pilot country will be invited to appoint 2-3 experts who will then participate in different project activities.

OBJECTIVE, OUTCOMES AND ACTIVITIES

Impact	To enhance cooperation on cybercrime and electronic evidence between Member States of the European Union and other Parties to the Budapest Convention on Cybercrime.
Project objective	To contribute to the ratification and implementation by EU Member States of the Second Additional Protocol to the Budapest Convention on Cybercrime. Objectively verifiable indicators for this action will include: – Number of signatures and status of ratification of the Second Additional Protocol by EU m/s. – Quality of (draft) laws and regulations implementing the Protocol. – Increased capacities of practitioners in pilot countries to apply the Second Protocol. – Up-to-date online resources for practitioners implementing the Second Protocol.
Outcome 1	Increased alignment of domestic legislation of EU Member States with the Second Protocol. Objectively verifiable indicators: – Number of EU m/s undertaking reforms to align domestic legislation and regulations with the requirements of the Second Protocol. – Number of EU m/s that have completed reforms or have prepared drafts of domestic legislation and regulations.
Output 1.1	Authorities EU m/s are engaged in a process of reform of domestic legislation and regulations.
Activities	
	Identify counterparts in EU m/s responsible for implementing the Second Protocol in domestic law.
	Identify 5 EU m/s that are ready to function as pilot countries for the implementation of the Second Protocol.
	Prepare a guide or manual on the interaction between the Second Protocol and other instruments, including the E-evidence Regulation and Directive.
	Bi-monthly online progress meetings with counterparts of all EU m/s. Consider meetings back-to-back with meetings convened by the EU Commission on implementation the E-evidence Regulation.
	Meetings (workshops, roundtables) with counterparts in pilot countries
	Meetings, briefings and consultations with members of parliaments on the Second Protocol (online, in person, national and regional).

Output 1.2	Draft legislative and other measures are available in EU m/s implementing the provisions of the Second Protocol.
Activities	
	Prepare guides, legal profiles and other resources on legislation and other measures to facilitate implementation of the Second Protocol in domestic law (in cooperation with the Sirius Project).
	Workshops, round tables and other forms of advice to counterparts in pilot m/s preparing legislative amendments.
	Support/advice to EU m/s on domestic reforms on request.
Outcome 2	EU Member States are signatories and have made progress towards becoming Parties to the Second Protocol. Outcomes/objectively verifiable indicators: – Number of signatories to the Second Protocol. – Status of ratification process to the Second Protocol.
Output 2.1	EU m/s are signatories to the Second Protocol.
Activities	
	Hold a launching conference of the project to confirm engagement by EU m/s to undertake the necessary reform of domestic legislation in view of becoming Parties to the Second Protocol.
	Support Ireland in the ratification of the Convention on Cybercrime to permit subsequent signature of the Second Protocol.
	Engage in dialogue with T-CY representatives, Permanent Representations and other relevant authorities in those EU m/s that have not yet signed the Second Protocol.
	Create treaty events to facilitate signature of the Second Protocol.
Output 2.2	EU m/s have made measurable progress towards becoming Parties to the Second Protocol.
Activities	
	Hold bi-monthly online progress meetings with T-CY representatives and counterparts responsible for ratification of the Second Protocol.
	Hold meeting with decision makers in pilot m/s.
	Create treaty events to facilitate ratification of the Second Protocol.
	Hold meetings with counterparts from all EU m/s to exchange information on reforms underway.
	Hold a project closing event to assess results achieved.
Outcome 3	Improved capacities of criminal justice practitioners in EU m/s to apply the tools of the Second Protocol. Outcomes/objectively verifiable indicators: – Number of training sessions and participants trained. – Number of exercises held and participants engaged.
Output 3.1	Competent criminal justice authorities of EU m/s are able to apply the tools of the Second Protocol.
Activities	
	Develop and deliver training courses on the tools of the Second Protocol in person and through the online training platform of the C-PROC and in cooperation with EUROJUST, EUROPOL and CEPOL.

	Develop guides and templates for government-to-government cooperation (in cooperation with the SIRIUS Project).
	Support the establishment and training of authorities to be declared under articles 6.6, 7.5, 8.10, 14.7.c and 14.10.b of the Second Protocol.
	Support procedures and deliver training on – emergency disclosure (article 9) for 24/7 points of contact, and – emergency mutual assistance (Article 10) for central authorities and other authorities responsible for mutual assistance and prepare an informal directory of authorities for the purposes of Article 10.5 (see ER 77).
	Revision and roll-out of the updated HELP Online Course on cybercrime and electronic evidence with focus on Modules for international cooperation and the Second Protocol.
	Support conferences and other events between competent authorities of EU m/s and other Parties to the Convention.
Output 3.2	Increased public/private cooperation across borders on the basis of the Second Additional Protocol.
Activities	
	Develop practical guides, procedures and templates for competent authorities, service provides and registrars in EU m/s for the application of articles 6 (requests for domain name registration information) and 7 (production orders for subscriber information) of the Second Protocol, including the notification regime under article 7.5.
	Prepare inventories/manuals of provider policies with respect to languages of orders (Article 3, ER 61), WHOIS (ER 84.d), notification (ER 106) and confidentiality (ER 165) policies (in cooperation with SIRIUS).
	Hold practical exercises with criminal justice authorities and service providers and entities on articles 6 and 7 (pilot m/s, all EU m/s, all Parties).

CONTACT

Cybercrime Programme Office of the
Council of Europe (C-PROC)
Bucharest, Romania
cybercrime@coe.int
www.coe.int/cybercrime