www.coe.int/cybercrime

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Strasbourg, 9 September 2025

T-CY (2025)10

Cybercrime Convention Committee (T-CY)

Assessment of the search and seizure of stored computer data (Article 19 of the Budapest Convention)

Questionnaire on follow up given by Parties to Recommendations on the implementation of Article 19 of the Budapest Convention adopted in December 2024

Draft version for consideration by the 33rd T-CY Plenary (13-14 November 2025)

Background:

The purpose of this questionnaire is to enable the T-CY Plenary to review the follow-up provided by Parties to the Budapest Convention regarding the Recommendations on the implementation of Article 19 of the Budapest Convention, adopted by the T-CY in December 2024. The T-CY had agreed that:

"Parties are invited to provide an update on follow up to applicable recommendations falling under the responsibility of domestic authorities to report back to the T-CY no later than 18 months from adoption of this report on measures taken to permit the T-CY, in line with the Rules of Procedure (Article 2.1.g), to review progress made."

Recommendations 1 to 16 were considered "falling primarily under the responsibility of domestic authorities".

Implementation:

T-CY representatives are invited to prepare/compile consolidated replies to this questionnaire from their respective country and submit them no later than **30 June 2026** in electronic form in English or French to T-CY.secretariat@coe.int.

The Bureau will then provide an initial summary to T-CY 35 (end 2026), and a full draft report by spring 2027 for consideration by T-CY 36 (mid-2027).

Question 1: Please provide information on measures taken, initiatives, or on relevant developments in relation to the following Recommendations. You may also attach supporting documents illustrating progress, as appropriate (e.g., laws, policies, guidance documents, case law, reports, statistics, etc.).

Rec 1	Parties should ensure that powers of search and seizure are sufficiently detailed and specific to meet the requirements of Article 19 of the Convention. To the extent that the elements of Article 19 cannot be fulfilled by using general or "traditional" procedural powers (such as those that pertain to house searches or the seizure of tangible objects) objects), Parties should give due consideration to establishing powers and procedures specific to stored computer data to meet these obligations. Such specific provisions could also provide greater clarity and enhance legal certainty. Parties may also provide (for example by standard operating procedures or similar guidelines) that judicial authorisations for searches and seizures pertain to specified computer systems or data in order to apply the conditions and safeguards of Article 15.
Measures taken/relevant developments:	
Rec 2	Parties that do not provide for definitions of computer data (covering computer data, traffic data, subscriber information) in their domestic laws are encouraged to do so based on the relevant definitions contained in the Convention[1] and apply the powers of search and seizure of stored computer data to all types of computer data (subscriber information, traffic and content data) in their stored form.
Measures taken/relevant developments:	
Rec 3	Parties are encouraged to establish clear guidance for national authorities about how to deal with certain specific situations they may encounter in practice when accessing and securing computer data to ensure a consistent approach, where possible, at domestic level for similar situations. Such situations might include 1) an unopened email message waiting in the mailbox of a service provider until the addressee downloads it, as referred to in para 190 of the Explanatory Report to the Convention, 2) search and seizure of virtual assets or 3) obtaining data in volatile memory or triage procedures when multiple physical devices are found.
Measures taken/relevant developments:	
Rec 4	Parties should consider providing for continuous training and guidance of their competent authorities that authorise and carry out search and seizure (including joint trainings for judges, prosecutors and law enforcement officials), especially given the increasing complexity of emerging technologies and how data can be used as electronic evidence of crime. Such training may be complemented by the adoption of guidance documents, where appropriate. Such training activities may be supported, if desired by the Party, by the capacity building programmes of the Council of Europe.

[1] This is without prejudice to paragraph 22 of the Explanatory Report.

Measures taken/relevant developments:	
Rec 5	Parties are encouraged to explicitly provide in their legislation for the different conditions and requirements set out in Article 19.2 of the Convention.
Measures taken/relevant developments:	
Rec 6	Parties should ensure that they have the power to copy data when accessing a computer system. This measure may be preferable to seizing an entire computer system in certain situations (for example, where the data being searched or similarly accessed may be stored on the computer system of a witness who is not actually involved in the wrongdoing or where the data is on a server of a service provider).
Measures taken/relevant developments:	
Rec 7	In their domestic law or in internal standard operating procedures or similar guidelines, Parties should specify requirements related to maintaining the integrity of the data and chain of custody to ensure that the data were not interfered with (protocols of actions, creating images, hash values, data storage, retention periods). Some of these elements may be found in Article 14 of the Second Additional Protocol (for example quality and integrity, retention periods, data security, etc.).
Measures taken/relevant developments:	
Rec 8	Parties should ensure that they have the power to remove the data from a searched computer system or to render them inaccessible under certain conditions.
Measures taken/relevant developments:[2]	
Rec 9	Parties should ensure that they have the power to order any person with knowledge about the functioning of a computer system, or measures applied to protect its data, to provide, as is reasonable, the information necessary to carry out the actions in Article 19. Amendment of statutes and investigative practices in this respect is urgent Without prejudice to certain rights under their domestic laws (for example, the right against self-incrimination), Parties are encouraged to consider establishing sanctions if the person refuses to provide necessary cooperation. Parties should restrict the use of this power to provision of information that is reasonable. In particular, Parties should avoid using this power where the disclosure of the password or other security measure would unreasonably threaten the privacy of other users or other data that is not authorised to be searched. In such cases, the provision of the "necessary information" could be the disclosure, in a form that is intelligible and readable, of the actual data that is being sought by the competent authorities.

[2] Completion of this field is only requested if information has not been provided to the T-CY before (See document T-CY(2016)13).

Measures taken/relevant developments:	
Rec 10	In the same vein, Parties are encouraged to specify in their domestic law or in internal standard operating procedures or similar guidelines: - grounds that must be met or steps that must be taken to acquire credentials lawfully in accordance with the domestic law of a Party; - how lawfully acquired credentials may be used by their competent authorities for example, for downloading stored computer data, for undercover activities when controlling the account, or for changing credentials, etc.).
Measures taken/relevant developments:	
Rec 11	Parties should ensure that their powers to search and seize computer data extend to all types of crimes, consistent with the scope of the Convention under Article 14. In countries where these powers derive from a combination of statutes, the interplay of these statutes should be examined for cases that would fall outside all statutes.
Measures taken/relevant developments:	
Rec 12	Consistent with obligations under Article 15, Parties should ensure that the measures of search and seizure are applied in accordance with the principle of proportionality, in accordance with relevant principles of their domestic law. The Parties are to apply the conditions and safeguards regardless of whether the power of search and seizure is carried out at the location where the computer system or data is found, or in or from another place. Parties should ensure that applicable legal privileges and immunities are protected. This may include the ability to seek redress for persons claiming such protection. When applying measures of Article 19, to the extent consistent with the public interest, Parties should consider their impact on the rights, responsibilities and legitimate interests of third parties, including service providers, and whether appropriate means can be taken to mitigate such impact.
Measures taken/relevant developments:	
Rec 13	Some Parties do not have any existing systems in place for conducting searches and seizures of systems consistent with Article 19 in emergency or urgent situations, or they have basic, informal, or ad hoc systems. These Parties are encouraged to review the present Assessment Report to learn how other Parties have approached these situations before they are confronted with an actual emergency or urgency. Parties with more robust systems in place are similarly encouraged to review this Assessment to determine if other Parties may have elements useful to incorporate into their own system. All Parties are reminded that the Second Additional Protocol provides a definition of "emergency" that may provide useful guidance.
Measures taken/relevant developments:	

Rec 14	Extension of searches to a location known to be foreign or to an unknown location has become an urgent issue that practitioners face. Therefore, Parties should prepare their positions on extensions of searches from their own territory to a location known to be foreign or to an unknown location. In developing such positions, Parties should consider the possible implications of an extension of searches cross border (policy, legal and other considerations, including the rights of individuals and third parties as well as potential invalidation and suppression of evidence). Possible second judicial authorisations, consultation with or notification of the targeted country, awareness raising for competent authorities, and amendments to domestic law could be considered in order to mitigate the risks.
Measures taken/relevant developments:	
Rec 15	Although the measures of extension of searches outside of the territory of a Party or to an unknown location and covert remote access are not specifically provided for in the Convention, Parties may ensure that such measures are subject to the conditions and safeguards that are provided for in Article 15 of the Convention.
Measures taken/relevant developments:	
Rec 16	Where appropriate, Parties are encouraged to consider sharing their internal standard operating procedures or similar guidelines on the implementation of Article 19 with the Secretariat to make them available with restricted access on the recently developed online platform for exchange of materials, training, and resource sharing on cybercrime and electronic evidence (CYBOX).
Measures taken/relevant developments:	

Question 2: Additional information (as appropriate)

Please provide any other relevant information, developments, good practices, or lessons learned since the assessment of Article 19. You may also attach supporting documents, if available (e.g. laws, policies, guidance documents, case law, reports, statistics, etc.).
Party's response: