
Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings

(Adopted by the Committee of Ministers on 30 January 2019, at the 1335th meeting of the Ministers' Deputies)

The Committee of Ministers,

Considering that the aim of the Council of Europe is to achieve a greater unity between the member States, in particular by promoting the adoption of common rules in legal matters;

Considering the necessity of providing practical guidance for the handling of electronic evidence in civil and administrative proceedings to courts and other competent authorities with adjudicative functions; professionals, including legal practitioners; and parties to proceedings;

Considering that these guidelines seek to provide a common framework rather than a harmonisation of the national legislation of the member States;

Considering the need to respect the diversity in the legal systems of the member States;

Acknowledging the progress made in the member States towards the digitisation of their justice systems;

Noting, nonetheless, obstacles to the effective management of electronic evidence within justice systems, such as the lack of common standards and the diversity and complexity of evidence-taking procedures;

Highlighting the need to facilitate the use of electronic evidence within legal systems and in court practices;

Recognising the need for member States to examine current deficiencies in the use of electronic evidence and to identify the areas where electronic evidence principles and practices could be introduced or improved;

Noting that the aim of these guidelines is to provide practical solutions to the existing deficiencies in law and practice,

Adopts the following guidelines to serve as a practical tool for the member States, to assist them in adapting the operation of their judicial and other dispute-resolution mechanisms to address issues arising in relation to electronic evidence in civil and administrative proceedings, and invites them to disseminate these guidelines widely with a view to their implementation by those responsible for, or otherwise handling, electronic evidence.

Purpose and scope

The guidelines deal with:

- oral evidence taken by a remote link;

- use of electronic evidence;
- collection, seizure and transmission of evidence;
- relevance;
- reliability;
- storage and preservation;
- archiving;
- awareness-raising, review, training and education.

The guidelines are not to be interpreted as prescribing a specific probative value for certain types of electronic evidence and are to be applied only insofar as they are not in conflict with national legislation.

The guidelines aim to facilitate the use and management of electronic evidence within legal systems and in court practices.

Definitions

For the purposes of these guidelines:

Electronic evidence

“Electronic evidence” means any evidence derived from data contained in or produced by any device, the functioning of which depends on a software program or data stored on or transmitted over a computer system or network.

Metadata

“Metadata” refers to electronic information about other electronic data, which may reveal the identification, origin or history of the evidence, as well as relevant dates and times.

Trust service

“Trust service” means an electronic service which consists of:

- a. the creation, verification and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services; or
- b. the creation, verification and validation of certificates for website authentication; or
- c. the preservation of electronic signatures, seals or certificates related to those services.

Court

The term “court” includes any competent authority with adjudicative functions in the performance of which it handles electronic evidence.

Fundamental principles

It is for courts to decide on the potential probative value of electronic evidence in accordance with national law.

Electronic evidence should be evaluated in the same way as other types of evidence, in particular regarding its admissibility, authenticity, accuracy and integrity.

The treatment of electronic evidence should not be disadvantageous to the parties or give unfair advantage to one of them.

Guidelines

Oral evidence taken by remote link

1. Oral evidence can be taken remotely, using technical devices, if the nature of the evidence so permits.
2. When deciding whether oral evidence can be taken remotely, the courts should consider, in particular, the following factors:
 - the significance of the evidence;
 - the status of the person giving evidence;
 - the security and integrity of the video link through which the evidence is to be transmitted;
 - costs and difficulties of bringing the relevant person to court.
3. When taking evidence remotely, it is necessary to ensure that:
 - a. the transmission of the oral evidence can be seen and heard by those involved in the proceedings and by members of the public where the proceedings are held in public; and
 - b. the person being heard from a remote location is able to see and hear the proceedings to the extent necessary to ensure that they are conducted fairly and effectively.
4. The procedure and technologies applied to the taking of evidence from a remote location should not compromise the admissibility of such evidence and the ability of the court to establish the identity of the persons concerned.
5. Irrespective of whether evidence is transmitted via a private or a public connection, the quality of the videoconference should be ensured and the video signal encrypted to protect against interception.

Use of electronic evidence

6. Courts should not refuse electronic evidence and should not deny its legal effect only because it is collected and/or submitted in an electronic form.
7. In principle, courts should not deny the legal effect of electronic evidence only because it lacks an advanced, qualified or similarly secured electronic signature.
8. Courts should be aware of the probative value of metadata and of the potential consequences of not using it.
9. Parties should be permitted to submit electronic evidence in its original electronic format, without the need to supply printouts.

Collection, seizure and transmission

10. Electronic evidence should be collected in an appropriate and secure manner, and submitted to the courts using reliable services, such as trust services.
11. Having regard to the higher risk of the potential destruction or loss of electronic evidence compared to non-electronic evidence, member States should establish procedures for the secure seizure and collection of electronic evidence.
12. Courts should be aware of the specific issues that arise when dealing with the seizure and collection of electronic evidence abroad, including in cross-border cases.

13. Courts should co-operate in the cross-border taking of evidence. The court receiving the request should inform the requesting court of all the conditions, including restrictions, under which evidence can be taken by the requested court.
14. Electronic evidence should be collected, structured and managed in a manner that facilitates its transmission to other courts, in particular to an appellate court.
15. Transmission of electronic evidence by electronic means should be encouraged and facilitated in order to improve efficiency in court proceedings.
16. Systems and devices used for transmitting electronic evidence should be capable of maintaining its integrity.

Relevance

17. Courts should engage in the active management of electronic evidence in order, in particular, to avoid excessive or speculative provision of, or demand for, electronic evidence.
18. Courts may require the analysis of electronic evidence by experts, especially when complex evidentiary issues are raised or where manipulation of electronic evidence is alleged. Courts should decide whether such persons have sufficient expertise in the matter.

Reliability

19. As regards reliability, courts should consider all relevant factors concerning the source and authenticity of the electronic evidence.
20. Courts should be aware of the value of trust services in establishing the reliability of electronic evidence.
21. As far as a national legal system permits, and subject to the court's discretion, electronic data should be accepted as evidence unless the authenticity of such data is challenged by one of the parties.
22. As far as a national legal system permits, and subject to the court's discretion, the reliability of the electronic data should be presumed, provided that the identity of the signatory can be validated and the integrity of the data secured, unless and until there are reasonable doubts to the contrary.
23. Where applicable law provides special protection for categories of vulnerable persons that law should have precedence over these guidelines.
24. As far as a national legal system so provides, where a public authority transmits electronic evidence independently of the parties, such evidence is conclusive as to its content, unless and until proved to the contrary.

Storage and preservation

25. Electronic evidence should be stored in a manner that preserves readability, accessibility, integrity, authenticity, reliability and, where applicable, confidentiality and privacy.
26. Electronic evidence should be stored with standardised metadata so that the context of its creation is clear.
27. The readability and accessibility of stored electronic evidence should be guaranteed over time, taking into account the evolution of information technology.

Archiving

28. Courts should archive electronic evidence in accordance with national law. Electronic archives should meet all safety requirements and guarantee the integrity, authenticity, confidentiality and quality of the data as well as respect for privacy.
29. The archiving of electronic evidence should be carried out by qualified specialists.
30. Data should be migrated to new storage media when necessary in order to preserve accessibility to electronic evidence.





Awareness-raising, review, training and education

31. Member States should promote awareness of the benefits and value of electronic evidence in civil and administrative proceedings.
32. Member States should keep technical standards related to electronic evidence under review.
33. All professionals dealing with electronic evidence should have access to the necessary interdisciplinary training on how to handle such evidence.
34. Judges and legal practitioners should be aware of the evolution of information technologies which may affect the availability and value of electronic evidence.
35. Legal education should include modules on electronic evidence.

Related documents


CM/Del/Dec(2019)1335/10.1

European Committee on Legal Co-operation (CDCJ) - a. Report of the 93rd plenary meeting (Strasbourg, 14-16 November 2018) - b. Draft guidelines of the Committee of Ministers on electronic evidence in civil and administrative proceedings and their explanatory memorandum

 DOCX  30/01/2019  English  CM-Public




CM(2018)169

European Committee on Legal Co-operation (CDCJ) - a. Report of the 93rd plenary meeting (Strasbourg, 14-16 November 2018) [1335 meeting]

 DOCX  17/12/2018  English  CM-Public

CM(2018)169-add2

European Committee on Legal Co-operation (CDCJ) - b. Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings - Explanatory Memorandum [1335 meeting]

 DOCX  17/12/2018  English  CM-Public

1335th meeting of the Ministers' Deputies (30 January 2019) ... 20/11/2018

www.coe.int/.../january-2019?p_p_id=101_INSTANCE_FJJuJash2rEF&p...

17 January 2019 - Meeting - GR-J - Meetings and events - Jan... 20/11/2018

www.coe.int/.../january-2019?p_p_id=101_INSTANCE_FJJuJash2rEF&p...

Sign In - Please click here to login and see classified information.