ELECTRONIC EVIDENCE IN CIVIL AND ADMINISTRATIVE PROCEEDINGS

Legal instruments

Guidelines
and explanatory memorandum

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

ELECTRONIC EVIDENCE IN CIVIL AND ADMINISTRATIVE PROCEEDINGS

Guidelines
adopted by the Committee of Ministers
of the Council of Europe
on 30 January 2019
and explanatory memorandum

Council of Europe

French edition:

Preuves électroniques dans les procédures civiles et administratives (Lignes directrices et exposé des motifs)
ISBN 978-92-871-8928-8

Cover design and layout:
Documents and Publications Production Department (SPDP), Council of Europe

Council of Europe
F-67075 Strasbourg Cedex
http://book.coe.int

ISBN 978-92-871-8929-5

Printed at the Council of Europe

The Guidelines of the Committee of Ministers to member States on electronic evidence in civil and administrative proceedings were adopted by the Committee of Ministers of the Council of Europe on 30 January 2019, as proposed by the European Committee on Legal Co-operation (CDCJ).

This publication contains the text of the guidelines and their explanatory memorandum.

Contents

GUIDELINES		**5**
EXPLANATORY MEMORANDUM		**13**
	General comments	13
	Working method and the drafting process	13
	Preamble	14
	Purpose and scope	14
	Definitions	15
	Fundamental principles	16
	Guidelines	17
	Selected bibliography and other sources	28

Guidelines

of the Committee of Ministers to member States 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.

Explanatory memorandum

General comments

Why do we need a new instrument?

1. Courts are being increasingly called upon to handle electronic evidence or to authorise the production of electronic data by parties and other persons involved in civil or administrative proceedings.

2. To date, there are few standards for electronic evidence at international, European or national levels. Significant deficiencies remain in the law and practice concerning electronic evidence.

3. The purpose of these guidelines on electronic evidence is not to establish binding legal standards, but rather to serve as a practical tool for Council of Europe member States when adapting the operation of their judicial and other dispute-resolution mechanisms to address issues arising in relation to electronic evidence. In this respect, the guidelines are intended to strengthen the efficiency and quality of justice.

4. Electronic evidence differs in many respects from other types of evidence, and courts and other competent authorities with adjudicative functions are faced with specific challenges when dealing with this evidence. These challenges underline the need to enhance knowledge about electronic evidence and to improve how it is handled in civil and administrative proceedings.

Working method and the drafting process

5. The issue of electronic evidence falls within the competence of the European Committee on Legal Co-operation (CDCJ) which is the Council of Europe intergovernmental body responsible for the Organisation's standard-setting activities in the field of public and private law, including civil and administrative law.

6. The guidelines were drawn up by a drafting group of CDCJ members and designated experts and are based on the proposals they made during the group meetings held in 2018. These meetings also involved relevant Council of Europe bodies with expertise and responsibilities in this field.

7. The drafting group took into consideration experience arising from the operation of electronic justice mechanisms existing in member States.

Examples from member States

- The electronic justice system – Lietuvos teismų informacinė sistema (LITEKO) – set up in **Lithuania** in 2004 reduces the number of paper files by allowing the parties to the proceedings to submit all procedural documents and monitor the progress of the case online.
- E-commercial and e-land registers and an integrated case-tracking system (eSpis) are under development in **Croatia**. eSpis will facilitate communication between parties to court proceedings and the court.

Structure and content

8. The guidelines are not only a declaration of principles. They also aim to provide practical advice.

Preamble

9. The preamble explains that the guidelines are to be applied only insofar as they do not contradict national legislation and that they are a non-binding instrument. They do not seek to harmonise the national legislation of the member States. The guidelines are not to be interpreted as prescribing a specific legal value for certain forms of electronic evidence. They are intended to be general enough to accommodate differences in the legal systems of the member States whose diversity is fully acknowledged.

Purpose and scope

10. The guidelines aim to ensure that specific challenges relating to electronic evidence are addressed, such as the potential probative value of metadata; the ease with which electronic evidence can be manipulated, distorted or erased; and the involvement of a third party (including trust service providers) in the collection and seizure of electronic evidence. The guidelines apply to the resolution of disputes in both civil and administrative proceedings.

Example from a member State

In **Slovakia**, administrative bodies are open to receiving electronic evidence based on the general rule that anything that has evidentiary value for the purpose of determining the actual state of affairs may be submitted as evidence, as long as such evidence is not obtained in violation of the law.

Definitions

Electronic evidence

11. The guidelines use a broad definition of "electronic evidence" (also known as "digital evidence"). It may take the form of text, video, photographs or audio recordings. Data may originate from different carriers or access methods, such as mobile phones, webpages, onboard computers or GPS recorders, including data stored in a storage space outside the party's own control. Electronic messages (e-mail) are a typical example of electronic evidence, as they originate from an electronic device (computer or computer-like device) and include relevant metadata (see the definition of "metadata" below).

Metadata

12. "Metadata" means data about other data, and is sometimes referred to as the "digital fingerprint" of electronic evidence. It may include important evidentiary data, such as the date and time of creation or modification of a file or document, or the author and the date and time when the data was sent. Metadata is usually not directly accessible.

Trust service

13. Trust services play a critical role in the identification, authentication and security of online transactions. The guidelines adopt the definition of "trust service" formulated in Article 3.16 of the Regulation (EU) No 910/2014 of the European Parliament and Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (the eIDAS Regulation). In the guidelines, reference is also made to specific trust services related to "simple", "advanced" or "qualified" electronic signatures and certificates, which implies the possible application of other definitions adopted in the eIDAS Regulation.

Court

14. A broad definition of "court" is used in order to cover all authorities which are competent to adjudicate legal disputes between parties to civil and administrative proceedings, such as courts, tribunals and administrative bodies.

Fundamental principles

15. The first principle explains that although the role of experts in the evaluation of electronic evidence is important, it is ultimately for the courts to decide on the potential probative value of this type of evidence. In doing so, courts may be bound by applicable law presumptions (for example, providing specific probative value for certain types of electronic evidence).

16. The second principle underlines that electronic evidence should be neither discriminated against nor privileged over other types of evidence. In this respect, courts should also adopt a neutral approach to technology. This means that any technology that proves the authenticity, accuracy and integrity of data should be accepted.

> European Court of Human Rights case law
>
> "While Article 6 of the Convention guarantees the right to a fair hearing, it does not lay down any rules on the admissibility of evidence or the way it should be assessed, which are therefore primarily matters for regulation by national law and the national courts." (see *García Ruiz v. Spain,* No. 30544/96, paragraph 28)

17. The third principle refers to the equality of arms and equal treatment of the parties to proceedings with regard to electronic evidence. Treatment of electronic evidence should not be disadvantageous to parties to civil or administrative proceedings. For example, a party should not be deprived of the possibility to challenge the authenticity of electronic evidence; or if a court only allows a party to submit electronic evidence in printout format, this party should not be deprived of the opportunity to submit relevant metadata to prove the reliability of the printout.

> European Court of Human Rights case law
>
> "[T]he principle of the equality of arms … implies that each party must be afforded a reasonable opportunity to present his case – including his evidence – under conditions that do not place him at a substantial disadvantage vis-à-vis his opponent." (see *Letinčić v. Croatia,* No. 7183/11, paragraph 48).

Guidelines

Oral evidence taken by remote link

18. Oral evidence taken by remote link is considered as electronic evidence for the purpose of these guidelines (see the definition of "electronic evidence" above). This section of the guidelines does not, however, cover pre-recorded oral evidence. It relates to oral evidence in the form of videoconferencing (transmission of synchronised image and sound in real time). Not all oral evidence can be taken by remote link. Attention must be given to the technical devices used to transmit oral evidence. It may be carried out remotely using analogue or digital technical devices enabling telecommunication transmission, in particular real-time, two-way communication allowing for the transmission of image and sound. If the testimony requires confidentiality, it may be necessary to apply measures or technical solutions to restrict access to the intelligible form of the secure communication to authorised persons only. Devices that ensure the integrity of telecommunications will provide the court and the parties an adequate and proper opportunity to challenge and question the "remote" witness.

Examples of regulations from the EU and a member State

- Article 10.4 of the Council Regulation (EC) No 1206/2001 of 28 May 2001 on co-operation between the courts of the member States in the taking of evidence in civil or commercial matters provides that the requesting court may ask the requested court to use communication technologies to take evidence, in particular by using videoconference and teleconference.
- Article 803 of the **Lithuanian** Code of Civil Procedure provides the possibility for the courts of the Republic of Lithuania to request a foreign court to use communication technologies (such as videoconferencing) to take evidence.

19. The decisive factors for whether oral evidence is taken by remote link are economic considerations (for example, reduction of the costs involved), practical difficulties (such as illness or disability of a witness) and procedural efficiency efforts to avoid excessive length of proceedings. If a person resides in a different country, it may be more appropriate to question him or her remotely. The same principle relates to a group of witnesses whose place of residence is distant from the judicial district of the court hearing the case. If a person is a key witness it may be more appropriate to question him or her in court. Other factors to be considered by the courts include participation and costs of translators for the hearing. It is important that judges, professionals, including legal practitioners, and court staff are aware of possible differences

between in-person testimony and remote testimony. For example, it is not as easy to observe and interpret the demeanour of witnesses during remote testimony.

20. These guidelines require that attention is paid to the process whereby the remote testimony is given. It is important to ensure that the technology used makes it possible to ask questions while the witness is giving testimony (if the rules of procedure so provide), particularly when the evidence is of fundamental importance for the resolution of the case. This requirement cannot be met when transmission is distorted due to weak connectivity or if access to the technical means is limited for the parties. This may give unfair advantage to one of the parties. As far as it is technically possible, the remote evidence should be taken in the same way as it is taken inside the court.

21. The methods used should properly secure image or sound transmission against loss, distortion or unauthorised disclosure. The court may verify the identity of the person giving testimony by requiring him or her to present an appropriate document, such as a valid identity card, passport or driving license.

22. All available systems of communication, both public and private, should ensure at minimum the quality of the videoconference and encryption of the video signal in order to protect against interception. It is possible to receive evidence via a private connection, if the national law permits, provided the solutions used offer enough technical security and respect procedural safeguards. A private connection in this context means a communication system that is not an official, governmental system specifically created for taking evidence in court.

Use of electronic evidence

23. Courts should be aware of the importance of electronic data being submitted by the parties as evidence in its original format. If a printout of electronic evidence is filed, the court may order, at the request of a party or on its own initiative, provision of the original of the electronic evidence by the relevant person. Geolocation data is an example of evidence that may have significant importance for resolving an issue, provided it is presented in original format. Most jurisdictions around the world have already expressly provided in their law for the use of electronic evidence in legal proceedings. Examples of such provisions can be found in the eIDAS Regulation.

Examples

The Supreme Court of **Croatia** (case No. I Kž 696/04-7) confirmed that SMS messages could be used as evidence in the proceedings as they were a source of information equal to any other written content stored on other media.

Example of technology to be specifically used for securing evidence: blockchain:

Blockchain is an emerging technology which has the potential to provide increased trust and security in electronic evidence. It can be defined as a distributed ledger that refers to the list of records (blocks) which are linked and secured using cryptography and are recorded in a decentralised peer-to-peer network. By design, a blockchain is inherently resistant to modification of the data. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires the agreement of the network majority. This makes blockchain suitable for evidencing purposes.

In the **USA**, § 1913 of the Vermont Rules of Evidence reads: "(1) A digital record electronically registered in a blockchain shall be self-authenticating pursuant to Vermont Rule of Evidence 902, if it is accompanied by a written declaration of a qualified person, made under oath, stating the qualification of the person to make the certification and: (a) the date and time the record entered the blockchain; (b) the date and time the record was received from the blockchain; (c) that the record was maintained in the blockchain as a regular conducted activity; and (d) that the record was made by the regularly conducted activity as a regular practice."

In **China**, in a judgment of 28 June 2018, the Hangzhou Internet Court ruled that in the case before it (an intellectual property dispute) data stored on a third-party blockchain platform was sufficiently reliable and free from interference that it could be relied upon and accepted by the court as evidence.

24. For the purposes of guideline 7, "advanced electronic signature" means an electronic signature which meets the requirements of Article 26 of the eIDAS regulation, namely *a*. it is uniquely linked to the signatory; *b*. it is capable of identifying the signatory; *c*. it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his or her sole control; and d. it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable. The term "qualified electronic signature" means an advanced electronic signature that has been created by a specific device for this purpose (a "qualified electronic signature creation device"). Such devices must benefit from a "qualified certificate for electronic signatures", that is a certificate that has been issued by a natural or legal person who provides one or more qualified trust services (a "qualified trust service provider") and who is authorised to do so by the appropriate supervisory body.

25. In current practice, most electronic data lacks advanced or qualified electronic signatures and is not secured in any other way. They should nevertheless still be considered by the courts as electronic evidence (while the probative value of the evidence may vary depending on the individual case) considering, for example, a variety of trust services related to electronic management of documents and identification of signatories that are available around the world. One example is the biometric signature, a method of obtaining an electronic version of a handwritten signature where a person writes his or her signature on an electronic device using a special pen and pad. Depending on the applicable law, the court may recognise such a biometric signature as equivalent to a handwritten signature on paper.

26. Metadata provides the necessary context to evaluate the evidence (data) in the same way as a postmark provides context for the evaluation of an ordinary (paper) letter and its content. Electronic evidence includes metadata as a matter of course and courts should be aware of its potential probative value. It can be used to trace and identify the source and destination of a communication, data on the device that generated the electronic evidence, the date, time, duration and the type of evidence. The metadata may be relevant, either as indirect evidence (such as indicating the most relevant version of the document) or as direct evidence (for example if the file data is manipulated). This guideline is also relevant in the case of lost metadata.

> Examples of case law on metadata in **Ireland**
>
> Metadata was considered important for authenticating the provenance of electronically created documents/materials (*Koger Inc. & Koger (Dublin) Ltd v. O'Donnell & Others* (2010) IEHC 350).
>
> The Irish Courts have ruled that there is an obligation for a party to civil proceedings to inform the other party (or parties) of electronically stored evidence that contain (discovery) the metadata of the native documents, where this would be relevant (*Sretaw v. Craven House Capital PLC* (2017) IEHC 580; *Gallagher v. RTE* (2017) IEHC 237).

27. Printouts of electronic evidence can be easily manipulated as they exclude metadata or other hidden data. Consequently, a screen printout from a web browser is not reliable evidence as it is nothing but a copy of the screen display. It can be modified in a very simple manner because no special software or hardware are required for this purpose.

> Example from a member State
>
> The Court of Appeal of **Lithuania** decided that instant copies of computer screen (screenshots) are not trustworthy (27 April 2018, Case No. e2A-226-516/2018).

Collection, seizure and transmission

28. Electronic evidence, by its very nature, is fragile and can be altered, damaged or destroyed by improper handling or examination. For these reasons, special precautions may be taken to properly collect this type of evidence. Failure to do so may render it unusable or lead to an inaccurate conclusion. In principle, the parties are responsible for the proper collection of electronic evidence in civil and administrative proceedings. Different types of data may require different methods of collection. Actions taken to secure and collect electronic evidence should not affect the integrity of that evidence. In matters of considerable importance, the parties should consider collecting the electronic evidence with the support of an IT specialist or notary services. Judges and professionals, including legal practitioners, should be aware that data is often stored using network-based services. This includes both cloud computing and the online delivery of services.

29. Judges and professionals, including legal practitioners, have increased their knowledge and expertise in handling electronic evidence, but specific standards are still missing. Collection and seizure of electronic evidence may require member States to adopt special tools and procedures. In the meantime, judges and professionals, including legal practitioners, should seek to ensure the integrity, confidentiality and security of such data. This includes the retention of secured backup copies should one of the means of storage fail. It is necessary to retain electronic data in its original format.

30. Although the use of data can be strictly national in nature, it is becoming more likely that it has a cross-border nature, involving other countries. An example is the location in another country of the infrastructure used for the processing or storage of the data, or of the provider that enables the storage or processing of the data. Direct co-operation between courts and trust or cloud service providers in cross-border cases is to be encouraged. When handling electronic evidence, judges and professionals, including legal practitioners, should take into consideration factors such as the place of establishment of the service provider, the place where the data is processed and the existence of local laws regulating access to the data.

> Example of cross-border technology
>
> Data sharing (clouds) is the storage of different parts of a database across various servers that might be located in different physical locations. This has become a common security technique. The global nature of the internet and the growing use of cloud services make it increasingly difficult to assume that access to data is strictly national in nature.

31. There are substantial differences between national procedural rules for the taking of evidence. Courts using evidence taken abroad should take those differences into consideration. It is recommended that in cross-border taking of electronic evidence, courts closely co-operate in this matter. A requesting court should be informed about the procedural rules used by the requested court in order to adapt their evaluation of the electronic evidence where appropriate. In particular, the taking of evidence abroad should not result in a violation of the basic principles and rights of procedural law, such as equality of arms.

32. The efficiency of the proceedings is improved when it is possible for electronic evidence to be transmitted to other courts in its original format rather than printing it and sending it out. Electronic data that is transmitted should be accompanied by its metadata. This includes use of additional metadata created by the courts for proper data-management purposes and its smooth transmission to other courts. Having structured metadata gives the courts control over the evidence. A copy of electronic evidence should ideally be used for transmission to another court.

33. Encouragement and facilitation of the transmission of electronic evidence by electronic means can be achieved through implementation of common technical standards and file formats, and by the digitisation of domestic judicial and administrative systems. Having regard to the higher risk of destruction of electronic evidence, procedures should be adopted at national level which permit the secure transmission of electronic evidence.

34. Data integrity, survivability and security should be taken into consideration when it comes to transmitting evidence. Reliable services, such as trust services, may be essential for ensuring the proper transmission of electronic evidence. If the transmission requires confidentiality, it may be necessary to apply measures or technical solutions, such as encryption, which restrict access to a secure communication to authorised persons only.

Relevance

35. Large amounts of unnecessary electronic evidence, which can be provided all too easily by a party, will make it difficult or impossible for the court and the other parties to handle it effectively. Therefore, active management of electronic evidence by the court, with a view to restricting its provision to what is strictly required to decide the case, is essential. The active management of data should respect the principle of proportionality. Every request to produce electronic evidence should be considered on its merits, in particular

its usefulness for probative purposes, and the parties should be entitled to challenge such requests.

36. Judges and professionals, including legal practitioners, should be aware of the possible need for technical expertise and recognise where further research or additional specialist knowledge, such as expert opinion, may be required. Experts must be competent and have sufficient training to undertake the assigned task.

Reliability

37. The separation of digital identity from physical identity may generate problems related to the reliability of the evidence. Courts should seek to establish the identity of the author of electronic data. If the applicable law does not specify the manner of establishing his or her identity, it may be determined in any objective way, such as electronic signature, or by checking the e-mail address from which the document was sent.

38. Trust services may provide technological mechanisms that ensure the reliability of evidence. For example, certificates to electronic signatures, sometimes referred to as the "digital ID" of a person, may guarantee both authenticity and integrity of the data. Where the identity of the signatory with an electronic signature is doubtful, a court may request the service provider related to the electronic signature to make a statement in relation to the matters upon which it is competent to provide evidence. Time-stamping (certification of time) may be equally important for evidencing the integrity of electronic data.

> Example of a trust service
>
> Time-stamping is a mechanism that makes it possible to prove the integrity of data. It demonstrates that data existed at a specific moment and has not been modified. The time-stamp is a valuable aspect of electronic evidence, as it includes relevant metadata about the moment of its creation.

39. As far as the applicable law allows for it, and subject to the court's discretion, the acceptance as evidence of all types of electronic evidence is encouraged and recommended for court practice. If there is a dispute, the parties generally identify the issues to be resolved, and unless a party raises the issue of the authenticity of the electronic evidence, the court does not need to raise the issue on its own initiative. The party seeking to rely on electronic evidence may be required to demonstrate its authenticity – for example by submitting metadata or seeking an appropriate legal order to obtain additional data from

other persons, such as trust services providers – only where a party challenges the electronic evidence.

40. The specific reference to the court's discretion in guidelines 21 and 22 underlines the important role of court discretion in respect of the subject matter of these guidelines.

41. As with any other type of evidence, a party to the proceedings may contest electronic evidence. In such cases, the said party may request the court to exclude the evidence, for example due to the fact that the author of the data cannot be properly identified. The reliability of electronic data may be proved in any manner, for example by qualified electronic signatures or other similar methods of identification that ensure integrity of the data. It is, however, for applicable law to define the legal effect of electronic signatures, for example by providing that only a qualified electronic signature should have the equivalent legal effect of a handwritten (wet ink) signature, or by requiring that the device used to generate the signature be under the exclusive control of the signatory.

EU qualified electronic signature

To ensure the integrity of data, courts do not need to carry out any specific analysis of the technology used for the creation of qualified electronic signatures. Checking the register of EU qualified trust service providers is sufficient.

42. Guideline 23 concerns the burden of proof. Consumers and vulnerable persons such as children may not be technically and/or economically able to provide electronic evidence. Where they benefit from statutory provisions that ease or reverse the burden of proof, those statutory provisions prevail over these guidelines. Courts should play an active role in cases where vulnerable persons are involved.

43. Depending on the national legal system, the evidential value of public (official) electronic systems that generate electronic evidence is to be respected. For example, data from electronic public registers can be treated as an official document, and therefore presumed to be reliable. An electronic recording of other proceedings may be treated as a reliable representation of the facts and free from the risk of human error (for example, when compared to content being dictated to a protocol by a judge).

Examples from the member States of public trust services

There are specific types of trust services made available at national level, such as "Trusted Profile" (**Poland**), "Electronic archiving and digitalisation" (**Belgium**),

"Information/documents long-term preservation, LEXNET Platform for exchanging information between the Judicial Bodies and a wide range of legal operators" (**Spain**).

Storage and preservation

44. Storage, within the meaning of these guidelines, refers to storage for the duration of the civil or administrative proceedings in question. Electronic evidence may be stored by the courts, for example, on portable devices (memory cards), servers, backup systems or other places for data storage (including cloud computing). Electronic evidence should be stored in its original format (i.e. not as printouts), in accordance with applicable law. Cybersecurity issues should also be taken into consideration, which means that courts should adopt proactive approaches to protecting the integrity of electronic evidence from cyberthreats, including damage or unauthorised access. By focusing on prevention, courts can prevent cyberthreats from affecting the integrity of electronic evidence and reduce overall cybersecurity risks. Regardless of the method used for storage, unauthorised individuals should not be given access to the electronic evidence.

45. Stored electronic evidence can be associated with standardised metadata describing the context of their creation and the existing links with other electronic records. The implementation of international standards for metadata ensures a level of consistency in storage of electronic evidence. As the creation of standardised metadata can be difficult and time consuming, courts may use tools that help generate the standardised metadata.

Example of a solution used to standardise metadata

A number of tools are available for the creation of standardised metadata. For example, the metadata management tool may generate an XML (eXtensible Markup Language) file containing the metadata related to the electronic evidence. XML files require no advanced professional software. It is both a standardised format and sufficiently flexible to be applied across different information systems. This tool may simplify both storage and retrieval of the electronic evidence.

In this regard, international standards applied to metadata should be followed, such as those published by organisations such as the International Organization for Standardization (ISO).

46. Guideline 27, concerning the preservation of electronic evidence, is applicable both to the storage and the archiving of electronic evidence that take place after completion of the proceedings. The electronic evidence should be stored and archived in the original form in which it was created, transmitted

and received and in a manner which does not materially change the data. The electronic evidence should be available in a readable format during the entire duration of the proceedings. The integrity of electronic evidence should be maintained at all stages.

Archiving

47. The guidelines on archiving cover the period after the proceedings and have regard to Recommendation Rec(2003)15 of the Committee of Ministers of the Council of Europe to member states on archiving of electronic documents in the legal sector. National law typically provides retention periods and technical archiving conditions. The systems employed for archiving need to be secure and guarantee traceable use and respect for privacy. Appropriate technical and organisational measures should be implemented in order to ensure the protection of electronic evidence, and to guard against unauthorised access to it. An electronic data carrier, if used, should be provided with an identification certificate containing basic data about it. Such a carrier should be properly protected, especially against loss, harmful effects of chemicals, heat, light, radiation, magnetic or electric fields and against mechanical damage.

48. Archiving services may verify, possibly using electronic signatures or other electronic procedures, that electronic evidence is being archived by qualified specialists or competent organisations and that data has not been altered by them. Both data on electronic signatures with which the electronic documents have been signed and data for verification of those signatures need to be properly archived. Member States should provide the organisations in the legal sector, entrusted by law with the duty of archiving, with the necessary resources for the archiving of electronic evidence.

49. Migration means changing the storage medium in order to preserve accessibility to electronic evidence. Neglect of migration may result in unreadability of the data. Electronic documents may be archived by periodic transfer of data from one storage medium to another or from one format to another. Migration should also apply to metadata concerning the archived electronic documents. Migration to a new storage medium should take place regularly, taking account of, for example, degradation and wear in the medium in question before they become obsolete, due to technological developments in the medium and hardware. Migration to a new storage medium or format should be carried out, when appropriate, in view of technological developments.

Example of a long-term solution

Data can be migrated to networked devices, such as cloud computing. These devices are being constantly improved as a result of the technological development in the medium and hardware. Cloud archiving may also provide greater control over cost by paying for only the space needed.

Example of an outdated solution

CDs, DVDs and other optical discs become unreadable due to physical or chemical deterioration. The causes vary from oxidation of the reflective layer, to physical scuffing and abrasion of disc surfaces or edges, including visible scratches, to other kinds of reactions with contaminants.

Awareness-raising, review, training and education

50. The promotion of these guidelines includes their wide dissemination to courts and legal practitioners, translation, and the organisation of seminars and conferences on electronic evidence.

51. Review of the technical standards related to electronic evidence may include, for example, new means of its storage, preservation and archiving.

52. Access to interdisciplinary training on handling electronic evidence is necessary for judges and professionals, including legal practitioners. Training may cover specific issues raised by electronic evidence, such as the importance of metadata and time-stamping, the use of cloud computing or blockchain in the collection and seizure of evidence and the need for submission of electronic evidence in its original format, rather than simply scanned images or printouts.

53. Awareness of the wider digital context and use of technologies such as cloud computing, trust services or blockchain is important for judges and professionals, including legal practitioners.

54. Instruction on material and procedural matters in the context of electronic evidence should be an essential part of legal education.

Selected bibliography and other sources

Albert J. (2013), "Study on possible national legal obstacles to full recognition of electronic processing of performance information on construction products (under the construction products regulation), notably within the regimes of civil liability and evidentiary value", European Commission, Final General Report, 30-CE-0517177/00-3630-CE-0517177/00-36.

Biasiotti M., Mifsud Bonnici J., Cannataci J. and Turchi F. (ed.) (2018), *Handling and Exchanging Electronic Evidence across Europe,* Springer International Publishing, Cham.

Biasiotti M. A., Turchi F. and Epifani M. (2015), "The EVIDENCE Project: Bridging the Gap in the Exchange of Digital Evidence Accross Europe", SADFE 2015, available at: http://bit.ly/31ZPA8I.

Capriolli E. (2007), *Droit international de l'économie numérique,* Paris, Litec.

Committee of Ministers (2003), Recommendation Rec(2003)15 of the Committee of Ministers of the Council of Europe to member states on archiving of electronic documents in the legal sector.

Forgó N., Hawellek C., Knoke F. and Stoklas J. (2017), "The Collection of Electronic Evidence in Germany – a Spotlight on Recent Legal Developments and Court Rulings" in *New Technology, Big Data and the Law,* Springer, Singapore.

Hofmann E., Strewe U. and Bosia N. (2018), *Supply Chain Finance and Blockchain Technology. The Case of Reverse Securitisation,* Springer, Munich.

International Telecommunication Union (2012), *Electronic Evidence: Model Policy Guidelines & Legislative Texts, Establishment of Harmonized Policies for the ICT Market in the ACP countries,* HIPCAR project "Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures", available at http://bit.ly/ITU-ElecEvid.

Mason S. (2016), *Electronic Signatures in Law,* Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London.

Mason S. (2016), *The use of electronic evidence in civil and administrative law proceedings and its effect on the rules of evidence and modes of proof. A comparative study and analysis,* report prepared by Stephen Mason assisted by Uwe Rasmussen, Strasbourg, 27 July 2016, CDCJ(2015)14-final.

Mason S. (2015), *Electronic Disclosure A Casebook for Civil and Criminal Practitioners,* PP Publishing 2015.

Mason S. (ed.) (2008), *International Electronic Evidence,* British Institute of International and Comparative Law, London.

Mason S. and Seng D. (ed.) (2017), *Electronic Evidence,* Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London.

Morabito V. (2017), *Business Innovation Through Blockchain. The B³ Perspective,* Springer International Publishing AG, Cham.

Schünemann W. and Baumann M. (ed.)(2017), *Privacy, Data Protection and Cybersecurity in Europe,* Springer International.

Singer P. and Friedman A. (2014), *Cybersecurity and cyberwar: What everyone needs to know,* Oxford University Press, Oxford.

Voigt P. and von dem Bussche A. (2017), *The EU General Data Protection Regulation (GDPR). A Practical Guide,* Springer International.

Sales agents for publications of the Council of Europe
Agents de vente des publications du Conseil de l'Europe

BELGIUM/BELGIQUE
La Librairie Européenne -
The European Bookshop
Rue de l'Orme, 1
BE-1040 BRUXELLES
Tel.: + 32 (0)2 231 04 35
Fax: + 32 (0)2 735 08 60
E-mail: info@libeurop.eu
http://www.libeurop.be

Jean De Lannoy/DL Services
c/o Michot Warehouses
Bergense steenweg 77
Chaussée de Mons
BE-1600 SINT PIETERS LEEUW
Fax: + 32 (0)2 706 52 27
E-mail: jean.de.lannoy@dl-servi.com
http://www.jean-de-lannoy.be

CANADA
Renouf Publishing Co. Ltd.
22-1010 Polytek Street
CDN-OTTAWA, ONT K1J 9J1
Tel.: + 1 613 745 2665
Fax: + 1 613 745 7660
Toll-Free Tel.: (866) 767-6766
E-mail: order.dept@renoufbooks.com
http://www.renoufbooks.com

CROATIA/CROATIE
Robert's Plus d.o.o.
Marasoviçeva 67
HR-21000 SPLIT
Tel.: + 385 21 315 800, 801, 802, 803
Fax: + 385 21 315 804
E-mail: robertsplus@robertsplus.hr

CZECH REPUBLIC/RÉPUBLIQUE TCHÈQUE
Suweco CZ, s.r.o.
Klecakova 347
CZ-180 21 PRAHA 9
Tel.: + 420 2 424 59 204
Fax: + 420 2 848 21 646
E-mail: import@suweco.cz
http://www.suweco.cz

DENMARK/DANEMARK
GAD
Vimmelskaftet 32
DK-1161 KØBENHAVN K
Tel.: + 45 77 66 60 00
Fax: + 45 77 66 60 01
E-mail: reception@gad.dk
http://www.gad.dk

FINLAND/FINLANDE
Akateeminen Kirjakauppa
PO Box 128
Keskuskatu 1
FI-00100 HELSINKI
Tel.: + 358 (0)9 121 4430
Fax: + 358 (0)9 121 4242
E-mail: akatilaus@akateeminen.com
http://www.akateeminen.com

FRANCE
Please contact directly /
Merci de contacter directement
Council of Europe Publishing
Éditions du Conseil de l'Europe
F-67075 STRASBOURG Cedex
Tel.: + 33 (0)3 88 41 25 81
Fax: + 33 (0)3 88 41 39 10
E-mail: publishing@coe.int
http://book.coe.int

Librairie Kléber
1, rue des Francs-Bourgeois
F-67000 STRASBOURG
Tel.: + 33 (0)3 88 15 78 88
Fax: + 33 (0)3 88 15 78 80
E-mail: librairie-kleber@coe.int
http://www.librairie-kleber.com

NORWAY/NORVÈGE
Akademika
Postboks 84 Blindern
NO-0314 OSLO
Tel.: + 47 2 218 8100
Fax: + 47 2 218 8103
E-mail: support@akademika.no
http://www.akademika.no

POLAND/POLOGNE
Ars Polona JSC
25 Obroncow Street
PL-03-933 WARSZAWA
Tel.: + 48 (0)22 509 86 00
Fax: + 48 (0)22 509 86 10
E-mail: arspolona@arspolona.com.pl
http://www.arspolona.com.pl

PORTUGAL
Marka Lda
Rua dos Correeiros 61-3
PT-1100-162 LISBOA
Tel: 351 21 3224040
Fax: 351 21 3224044
E mail: apoio.clientes@marka.pt
www.marka.pt

RUSSIAN FEDERATION/
FÉDÉRATION DE RUSSIE
Ves Mir
17b, Butlerova.ul. - Office 338
RU-117342 MOSCOW
Tel.: + 7 495 739 0971
Fax: + 7 495 739 0971
E-mail: orders@vesmirbooks.ru
http://www.vesmirbooks.ru

SWITZERLAND/SUISSE
Planetis Sàrl
16, chemin des Pins
CH-1273 ARZIER
Tel.: + 41 22 366 51 77
Fax: + 41 22 366 51 78
E-mail: info@planetis.ch

TAIWAN
Tycoon Information Inc.
5th Floor, No. 500, Chang-Chun Road
Taipei, Taiwan
Tel.: 886-2-8712 8886
Fax: 886-2-8712 4747, 8712 4777
E-mail: info@tycoon-info.com.tw
orders@tycoon-info.com.tw

UNITED KINGDOM/ROYAUME-UNI
The Stationery Office Ltd
PO Box 29
GB-NORWICH NR3 1GN
Tel.: + 44 (0)870 600 5522
Fax: + 44 (0)870 600 5533
E-mail: book.enquiries@tso.co.uk
http://www.tsoshop.co.uk

UNITED STATES and CANADA/
ÉTATS-UNIS et CANADA
Manhattan Publishing Co
670 White Plains Road
USA-10583 SCARSDALE, NY
Tel: + 1 914 472 4650
Fax: + 1 914 472 4316
E-mail: coe@manhattanpublishing.com
http://www.manhattanpublishing.com

Council of Europe Publishing/Éditions du Conseil de l'Europe
F-67075 STRASBOURG Cedex
Tel.: + 33 (0)3 88 41 25 81 – Fax: + 33 (0)3 88 41 39 10 – E-mail: publishing@coe.int – Website: http://book.coe.int

The *Guidelines on electronic evidence in civil and administrative proceedings* have been designed to serve as a practical tool to facilitate the use of this type of evidence in court proceedings. Their primary purpose is to help the Council of Europe member States to adapt the operation of their dispute-resolution mechanisms in order to address issues arising in relation to electronic evidence in civil and administrative proceedings, and in so doing strengthen the efficiency and quality of justice.

The guidelines deal with oral evidence taken by a remote link; the use of electronic evidence; collection, seizure and transmission of evidence; relevance; reliability; storage and preservation; archiving; awareness-raising; the review of relevant technical standards; and training and education.

They constitute the first international instrument in the field.

PREMS 021819

ENG

www.coe.int

The Council of Europe is the continent's leading human rights organisation. It comprises 47 member states, including all members of the European Union. All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states.

http://book.coe.int
ISBN 978-92-871-8929-5
€8/US$16

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE