CEELI INSTITUTE

ADVANCING THE RULE OF LAW

PRACTICAL GUIDELINES FOR REMOTE JUDGING IN CENTRAL AND EASTERN EUROPE

CEELI INSTITUTE

ADVANCING THE RULE OF LAW

The CEELI Institute is a Czech public-benefit (not-for-profit) organization based in Prague, dedicated to the development and training of an international network of legal and judicial professionals committed to advancing the rule of law. Through innovative training programs and other activities, the Institute works with judges, lawyers, and civil society actors to build laws-based societies. The CEELI Institute prides itself on the diversity and quality of the programs it has developed, the peer-to-peer exchanges it fosters, the innovative nature of its programming, and its legacy of contributing to the advancement of the rule of law in vulnerable countries. Our efforts are focused on creating independent, transparent, and effective judiciaries, strengthening democratic institutions, fostering efforts to combat corruption, bridging difficult conflicts, promoting human rights, and supporting lawyers and civil society actors in repressive environments. The CEELI Institute is based at the Villa Grébovka in Prague, a historic nineteenth-century building now renovated into a state-of-the-art residence and conference center.

PRACTICAL GUIDELINES FOR REMOTE JUDGING IN CENTRAL AND EASTERN EUROPE

Second edition
2022

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

The first version of this guide was developed by the CEELI Institute, the members of the Institute's Central and Eastern European Judicial Network, and the participants of the Institute's inaugural 'Remote Judging Certificate Course', held from late 2020 into early 2021. The second cohort of participants of the course from 2021 – 2022 have added some further insights and sections. The CEELI Institute wishes to thank the Working Group from this Course who conceived and drafted these Practical Guidelines on Remote Judging:

Judge Gjorgji Andonov, North Macedonia
Judge Shota Bichia, Georgia
Judge Ksenija Flack Makitan, Croatia
Judge Radoslava Kacherilska, Bulgaria
Judge Snežana Marjanović, Serbia
Andrej Bozinovski, North Macedonia

The working group for the second edition comprised;
Ms Tamar Chalidze, Georgia
Judge Betim Jahja, North Macedonia
Judge Tina Jakupak, Croatia
Judge Nenad Saveski, North Macedonia
Judge Vera Doborjginidze, Georgia

They worked on this document pro bono—without compensation, as a public service to support the work of judges.

Thanks also to Rachel Murray, Professor of International Human Rights Law at the University of Bristol (U.K.) and Director of its Human Rights Implementation Centre; Freda Grealy, Senior Program Manager at the CEELI Institute; Lilia Festa-Zaripova, Course Administrator at the CEELI Institute; and Malory Hudson and Maggie Utecht, CEELI Institute Legal Interns (William & Mary Law School) for their valuable contributions in developing these Guidelines.

This project was made possible by a grant and ongoing support from the U.S. Department of State's Bureau of International Narcotics and Law Enforcement Affairs (INL).

FOREWORD

The CEELI Institute has trained and supported judges in Central and Eastern Europe since 2000. These P*ractical Guidelines for Remote Judging in Central and Eastern Europe* were developed as part of the Institute's long-running Central and Eastern European Judicial Exchange Network. The Network, ongoing since 2012, is comprised of some of the best and brightest rising judges from twenty-one countries across the region who gather regularly to share best practices on issues of judicial independence, integrity, accountability, and court management.

In the face of the COVID-19 pandemic, judiciaries across the region and world were forced to rapidly adjust their daily operations. Many courts were forced to move quickly into the digital sphere. In response to this, the CEELI Institute sought ways to support judiciaries as they managed their pandemic response and their adjustment to use of new virtual platforms. We now seek to build off the experiences of the past eighteen months and use this opportunity to provide lasting guidance on remote judging practices which will remain relevant beyond the pandemic. We believe that the increased emphasis on technology and remote judging is here to stay. Promoting uses of technology that enhance the justice system and enable more efficient, timely, and accessible justice for all is a key responsibility of any modern judiciary.

With this mandate, the CEELI Institute has created this extended first edition of *Practical Guidelines for Remote Judging in Central and Eastern Europe.* This follows and complements an earlier edition of the Guidelines that was released by the CEELI Institute in April 2021. These *Guidelines* follow from our discussions with practicing judges during our training courses over the last year: *Best Practices for Remote Judging*, held online from Autumn 2020 through Spring 2021, and *Digital Justice in Central and Eastern Europe – Achieving Fairness, Accountability and Transparency*, held online April through June 2021. The Guidelines are the product of judicial innovation and adaption and reflect the experiences, discussions, and practices of our Network members over the past year. The goals of this document are to summarize current realities, provide realistic solutions, and offer practical tips in order to provide a framework for remote judging into the future. Remote judging is an integral part of the modern judiciary, and judges and practitioners will need to continue to adapt as these processes continue to evolve.

This document is relevant to individual judges and also to those responsible for developing policies and guidance for judicial practice, including members of judicial councils, court presidents, officials from judicial associations, and any other members of the judiciary who are responsible for regulating judges' work practices.

While drafting this document, the CEELI Institute and the Network judges referenced a wide range of materials and sources of information, including policies and recommendations by a number of international organizations. Finally, we note that these *Guidelines* are intended only as guiding principles and are not 'best practices.' While these *Guidelines* constitute a practical set of recommendations, it is important to stress that a judge's behaviour should always be in line with existing international standards, as well as national laws, regulations, and relevant guidance from judicial councils.

As noted, the CEELI Institute Judicial Exchange Network published a preliminary set of these *Guidelines* in April 2021, reflecting lessons learned during the initial stages of the pandemic. That document was in large part produced by the judges participating in our inaugural *Remote Judging Certificate course*. This new updated and expanded version of the *Guidelines* reflects the full range of experiences and practices developed by our Network judges over the past year. These *Guidelines* will be translated into regional languages. Please contact Freda.grealy@ceeli.eu if you have a particular request in this regard.

GLOSSARY

Recognising the variety of terms used by different jurisdictions and courts, this Glossary provides (unofficial) definitions for the terms referred to in this document.

- **Back-up system** – the process of duplicating files and system-specific, useful/essential data in case it is corrupted, deleted, or lost.
- **Bandwidth** – the speed of an internet connection, reflected in the amount of data that can be transmitted in a fixed amount of time. [1]
- **Break-out rooms** – functionality that enables the host to allocate participants to virtual rooms (i.e., other than the main hearing).[2]
- **Case management** – the system the court uses to lodge the files, store evidence, and exchange necessary written data between participants and the court.
- **Connection** – access to the internet that allows a user to participate in a video or audio meeting.[3]
- **Device** – electronic equipment used for communication purposes (e.g., phone, tablet, computer).[4]
- **Electronic evidence** – any probative information stored or transmitted in digital form.[5]
- **Electronic signature** – any type of signature in electronic format.[6]
- **Hearing** – a legal proceeding where an issue of law or fact is tried and evidence is presented to help determine the issue;[7] or formal examination of a cause, civil or criminal, before a judge, according to the laws of a particular jurisdiction.[8]

[1] Supreme Court of Victoria. 2021. Virtual Hearings Glossary. [online] Available at: https://www.supremecourt.vic.gov.au/law-and-practice/virtual-hearings/virtual-hearings-glossary

[2] Ibid.

[3] Ibid.

[4] Ibid.

[5] SHERLOC UNODC. 2021. Electronic Evidence. [online] Available at: https://sherloc.unodc.org/cld/topics/electronic-evidence/index.html?lng=en

[6] Cryptomathic. 2021. What is an electronic signature? [online] Available at: https://www.cryptomathic.com/products/authentication-signing/digital-signatures-faqs/what-is-an-electronic-signature

[7] The Free Dictionary. 2021. hearing. [online] Available at: https://legal-dictionary.thefreedictionary.com/hearing

[8] Encyclopedia Britannica. 2021. Hearing. [online] Available at: https://www.britannica.com/topic/hearing-law

- **Host** – the primary operator of a remote hearing.[9]
- **Hybrid hearing** – a hearing in which some of the participants are present in the courtroom (usually at least the judge) and others will join the hearing remotely via the internet from another location.
- **Live streaming** – the real-time broadcast of audio and/or video data (not recorded).
- **Mute/Unmute function** – when a microphone is turned off during a video or audio meeting. The microphone will not transmit any audio and the participant will not be heard by other participants.[10]
- **Platform** – a communications service (video and/or audio) that enables digital meetings via an email invitation or a telephone dial in (such as Zoom, Webex).[11]
- **Remote Hearing** – where judges, parties, legal representatives, and/or witnesses ('participants') do not gather physically at the same physical location; it normally involves some type of video link facility or telephonic mechanism,[12] sometimes also called an 'online' or 'virtual' hearing.[13]
- **Screen sharing** – sharing access to a given computer screen.[14]
- **Subpoena** – an order issued by the court; for example, a document compelling an individual to appear before the court.

9 Supreme Court of Victoria. 2021. Virtual Hearings Glossary. [online] Available at: https://www.supremecourt.vic.gov.au/law-and-practice/virtual-hearings/virtual-hearings-glossary

10 Supreme Court of Victoria. 2021. Virtual Hearings Glossary. [online] Available at: https://www.supremecourt.vic.gov.au/law-and-practice/virtual-hearings/virtual-hearings-glossary

11 Ibid.

12 Court of Judicature of Northern Ireland, Interim Practice Direction 01/2020 Remote Hearings, https://www.judiciaryni.uk/sites/judiciary/files/decisions/Practice%20Direction%2001-20.pdf; Michigan Legal Help. 2021. What To Expect at a Virtual Hearing. [online] Available at: https://michiganlegalhelp.org/self-help-tools/going-court/what-expect-virtual-hearing

13 OSCE Office for Democratic Institutions and Human Rights (ODIHR), Fair Trial Rights and Public Health Emergencies, 2021, https://www.osce.org/files/f/documents/3/8/487471_0.pdf; Supreme Court of Victoria. 2021. Virtual Hearings Glossary. [online] Available at: https://www.supremecourt.vic.gov.au/law-and-practice/virtual-hearings/virtual-hearings-glossary

14 See e.g., HM Courts & Tribunal Service. 2021. How to share documents in a Cloud Video Platform video hearing. [online] Available at: https://www.gov.uk/government/publications/how-to-join-a-cloud-video-platform-cvp-hearing/how-to-share-documents-in-a-cloud-video-platform-video-hearing#share-your-screen

ABBREVIATIONS

COE – Council of Europe

CCJE – Consultative Council of European Judges

CEPEJ – European Commission for the Efficiency of Justice

ECHR – European Convention on Human Rights

ECtHR – European Court of Human Rights

eIDAS – Electronic Identification Authentication and Trust Services

GDPR – General Data Protection Regulation

ICCPR – International Covenant on Civil and Political Rights

IT – Information technology

LAN – Local Area Network

OSCE/ODIHR – Organization for Security and Cooperation in Europe/Office of Democratic Initiatives and Human Rights

CHAPTER 1:
OPPORTUNITIES AND CHALLENGES IN REMOTE JUDGING

Remote judging is the holding of hearings or the conduct of other court business (including the exchange of evidence and documents) where one or more participants, including the judge, may not be physically present in person but participate through the use of technology or via electronic means. As the Organization for Security and Cooperation in Europe (OSCE) has noted: 'Such IT solutions include video platforms to conduct remote hearings, systems to enable the filing, dissemination and sharing of documents, digital case management and e-signatures. The use of such technology requires internet connectivity and data security, and access of court users to computers, cameras/webcams, microphones, screens and Wi-Fi.'[15]

Remote judging presents many opportunities:

- Digital technologies have the potential to ***increase the accessibility and effectiveness*** of justice systems, provided the principles of fairness, impartiality, and judicial independence are maintained.[16]

- New technologies ***connect people*** in different ways. The judge, litigants, lawyers, and witnesses are not physically present in the court room at the same time, but they are on an online platform together. Presence and the courtroom have new meanings.

- A remote hearing offers the potential to ***increase access to justice to parties*** who are not in the same location as the court, allowing them to directly participate in the proceedings. Remote hearings may be cheaper to conduct because the parties have no transportation costs, may need less time off from work, may require less attorney time, etc. Remote hearings also provide an opportunity to have a hearing which might otherwise not take place.

- A remote hearing could also ***enhance the credibility of the court***. Judges from within the same country could sit on cases no matter where they arise, thereby increasing the availability of judges with particular expertise.

- Remote hearings can more easily be conducted ***within a reasonable time***, thereby satisfying one of the components of the right to a fair trial.

- Remote hearings may be more ***cost-effective*** to the state, as less physical space may be needed for in-person hearings in the courthouse. They can be organised without or outside the courthouse, without involving some court employees (e.g., security officers).

---

15 OSCE Office for Democratic Institutions and Human Rights (ODIHR), *The functioning of courts in the Covid-19 pandemic. Primer*, October 2020, p.20.

16 *CEPEJ, European Judicial Systems, CEPEJ Evaluation Report*, 2020 Evaluation Cycle, https://rm.coe.int/evaluation-report-part-1-english/16809fc058

- It can simplify the exchange of documents. As the Consultative Council of European Judges (CCJE) noted: 'the parties and their representatives can access information about the cases in which they are involved before the court. In this way, they can follow the progress of their case by accessing the computerised case history.'[17]

- ***The mobility of the justice system*** can be enhanced with remote hearings. Remote hearings could allow for cases to be more evenly distributed among judges without regard to geographic location.

- Remote hearings have the potential to ***increase the transparency and monitoring of hearings by the public, the press, NGOs, and academic communities;*** video conferencing and live streaming, for example, can increase access to hearings by those monitoring the justice system.[18]

However, there are still practical challenges that courts face in remote judging:

- ***Remote judging may increase the risks to the right to a fair trial and standards of justice*** – Not all matters are suitable to be dealt with remotely. Relevant international standards on fair trials need to be upheld.

- ***Paper-based processes*** – In many jurisdictions, courts are still using paper as an official record, and wet signatures alongside authentication are still required. These courts are struggling with the burden of receiving, processing, storing, and moving documents.

- ***Requiring notarization***[19] ***can limit remote or virtual access to justice*** because of the costs involved and the complexity of the process.

- ***Moving from temporary to permanent solutions*** – During the emergency period, temporary rules allowed for digital processes; in many cases these provisions will not survive the pandemic. A compelling case would need to be made to move permanently away from paper-based processes and to provide remote options.

[17] Consultative Council of European Judges, Opinion No.14 of the CCJE *Justice and information technologies (IT)*, Adopted by the CCJE at its 12th plenary meeting (Strasbourg, 7-9 November 2011), https://rm.coe.int/168074816b, para 5.

[18] European Commission. 2021. *Digitalisation of justice.* [online] Available at: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/digitalisation-justice_en

[19] Notarization by a qualified Notary Public is an often-used method for providing authenticity of court documents and statements submitted by the parties.

CHAPTER 2:
INTERNATIONAL STANDARDS OF JUSTICE THAT MUST BE UPHELD

Checklist

International fair trial standards require that:

- ✓ Cases are heard by a competent, independent, and impartial tribunal established by the law
- ✓ Access to justice is assured
- ✓ Parties have a right to have their cause heard
- ✓ There is a right to a defence
- ✓ Defendants have a right to legal aid, in the interests of justice
- ✓ There is equality of arms
- ✓ Parties have a right to a public hearing
- ✓ Judgments must be pronounced publicly
- ✓ A hearing must be held within a reasonable time
- ✓ Parties have the right to an effective remedy
- ✓ Parties have the right to communicate freely and privately with their counsel

In criminal cases there are additional guarantees for the defendant:

- ✓ To be informed promptly and in detail in a language which they understand of the nature and cause of the charge against them
- ✓ To have adequate time and facilities for the preparation of their defence and to communicate with counsel of their own choosing
- ✓ To be tried in their presence and to defend themselves in person or through legal assistance of their own choosing
- ✓ To be informed of this right, if they do not have legal assistance

- ✓ To have legal assistance assigned to them in any case where the interests of justice so require, without payment by them in any such case if they do not have sufficient means to pay for it
- ✓ To examine, or have examined, the witnesses against them and to obtain the attendance and examination of witnesses on their behalf under the same conditions as witnesses against them
- ✓ To have the free assistance of an interpreter if they cannot understand or speak the language used in court

A. Minimum standards for fair hearings and access to justice

International instruments provide the minimum standards for fair hearings and for assuring access to justice. The right to a fair trial is set out in Article 14 of the International Covenant on Civil and Political Rights (ICCPR) and Article 6 of the European Convention on Human Rights (ECHR), as well as Article 47 of the Charter of Fundamental Rights of the European Union. These guarantees include the right:

- To a fair hearing within a reasonable time,
- By a competent, independent, and impartial tribunal established by law;
- In a public hearing.

Consistent with these provisions, everyone charged with a criminal offence shall have the following rights and minimum guarantees:

- To be presumed innocent until proven guilty according to law;
- To be informed promptly and in detail in a language which they understand of the nature and cause of the charge against them;
- To have adequate time and facilities for the preparation of one's defence and to communicate with counsel of one's choosing;
- To be tried without undue delay;
- To be tried in their presence and to defend themselves in person or through legal assistance of their own choosing; to be informed, if they do not have legal assistance, of this right; and to have legal assistance assigned to them in any case where the interests of justice so require, without payment by them in any such case if they do not have sufficient means to pay for it;
- To examine, or have examined, the witnesses against them and to obtain the attendance and examination of witnesses on their behalf under the same conditions as witnesses against them;
- To have the free assistance of an interpreter if they cannot understand or speak the language used in court;
- Not to be compelled to testify against oneself or to confess guilt;

[20] See also Venice Commission of the Council of Europe, *The Rule of Law Checklist,* Adopted by the Venice Commission at its 106th Plenary Session (Venice, 11-12 March 2016), https://www.venice.coe.int/images/SITE%20IMAGES/Publications/Rule_of_Law_Check_List.pdf

- Everyone convicted of a crime shall have the right to their conviction and sentence being reviewed by a higher tribunal according to law;

- No one shall be liable to be tried or punished again for an offence for which they have already been finally convicted or acquitted in accordance with the law and penal procedure of each country;

- The right to an effective remedy if rights are violated.

Any derogation from these rights must be temporary and subject to conditions of necessity and proportionality.[21] Even during a state of public emergency, the fundamental principle of the rule of law must prevail.

[21] Interim report on the measures taken in the EU member states, as a result of the Covid-19 crisis, and their impact on democracy, the Rule of law, and Fundamental rights adopted by the Venice Commission at its 124th online Plenary Session (8-9 October 2020) Opinion No. 995/2020 CDL-AD (2020)018, https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2020)018-e

B. Fair trial rights in the context of remote judging

With respect to the application of these rights in the context of remote judging, the European Court of Human Rights (ECtHR) has interpreted Article 6 of the ECHR in the context of remote hearings and proceedings as follows:

- Remote participation is not necessarily incompatible with the ECHR (*Sakhnovskiy v. Russia*, Grand Chamber, 2 November 2010),[22] but no party should be put at a substantial disadvantage (*Marcello v. Italy*, 5 October 2006).
- 'Physical presence may not be required as long as the court provides a right to present one's case effectively' (*Yevdokimov and Others v. Russia*, 16 February 2016).
- The importance of legal representation is crucial to fair hearings, although what is required varies by the circumstances of a case (*Vladimir Vasilyev v. Russia*, 10 January 2012).
- An individual must be able to follow proceedings (*Gorbunov and Gorbachev v. Russia*, 1 March 2016).
- There must be opportunity for private communication between a defendant and their lawyer (*Trepashkin v. Russia (no. 2)*, 16 December 2010).

[22] In regards to the use of a video link in the Sakhnovskiy case, the "Court reiterate[d] that this form of participation in proceedings is not… incompatible with the notion of a fair trial and public hearing. [However,] it must be ensured that the applicant is able to follow the proceedings and to be heard without technical impediments and that effective and confidential communication with a lawyer is provided for." It also noted that individuals charged with criminal offenses should "be entitled to be present at the first-instance trial hearing," but that attendance does not carry the "same significance for the appeal hearing."

Relevant Case Law from ECtHR on Article 6, European Convention on Human Rights

Sakhnovskiy v. Russia, Grand Chamber, 2 November 2010 *(Remote participation is not necessarily incompatible with the ECtHR).*
With regards to the use of a video link in the Sakhnovskiy case, the "Court reiterate[d] that this form of participation in proceedings is not… incompatible with the notion of a fair trial and public hearing. [However,] it must be ensured that the applicant is able to follow the proceedings and to be heard without technical impediments and that effective and confidential communication with a lawyer is provided for." It also noted that individuals charged with criminal offences should "be entitled to be present at the first-instance trial hearing," but that attendance does not carry the "same significance for the appeal hearing."

Marcello v. Italy (No.1), 5 October 2006 *(Physical presence may not be required but no party should be put at a substantial disadvantage).*
In Marcello v. Italy, the applicant argued that his participation via videoconference during appeal hearings was a violation of Article 6. The ECtHR highlighted that "in the interests of a fair and just criminal process it is of capital importance that the accused should appear at his trial" and "it is difficult to see how he could exercise [rights to defend himself in person, call and examine witnesses and have an interpreter] without being present." However, "personal appearance of the defendant does not take the same crucial significance for an appeal hearing as it does for the trial hearing," and the manner in which Article 6 ECHR applies in Court of Appeal instances depends on the special features of the proceedings as well as how the interests of the defence are presented and protected. Those proceedings "involving only questions of law, as opposed to questions of fact, may comply with the requirements of Article 6 even though the appellant was not given an opportunity of being heard in person." The court concluded that restrictions on an accused may be imposed if good cause exists, depending on whether they deprive the accused of a fair hearing in light of the entirety of the proceedings.

Yevdokimov and Others v. Russia, 16 February 2016 *(Physical presence may not be required as long as the court provides a right to present one's case effectively).*
The Yevdokimov case involved individuals who claimed violation of Article 6 ECHR on the basis that they had been unable to appear in person in court in civil proceedings where they were the parties. They were at that time in detention, and the domestic authorities refused their presence on the grounds that no legislation existed to bring detainees to court. The ECtHR held Article 6 "does not guarantee the right to personal presence before a civil court but enshrines a more general right to present one's case effectively before the court and to enjoy equality of arms with the opposing side," leaving it to the State to determine how the rights are guaranteed. The ECtHR further opined that "public hearing" means an entitlement to an "oral hearing," but this is not an absolute right and can be limited in exceptional circumstances – e.g., if facts

or law can be resolved on the basis of written materials. If an oral hearing has been provided at first instance, it may not be required on appeal. Where an individual is in custody, they could be represented by a lawyer in some circumstances. In this case, it found that "by failing to properly assess the nature of the civil claims brought by the applicants with a view to deciding whether their presence was indispensable and by focusing instead on deficiencies in the domestic law, and (ii) by failing to consider appropriate procedural arrangements enabling the applicants to be heard," there was a violation of Article 6.

Vladimir Vasilyev v. Russia, 10 January 2012 *(The importance of legal representation is crucial to fair hearings, although what is required varies by the circumstances of a case).*
Similar to the Yevdokimov case, Vladimir Vsilyev v. Russia involved an individual who claimed violation of Article 6 of the ECHR on the basis that he had been unable to appear in person in court for the civil proceeding in which he was a party. He was in detention at the time and not given the opportunity to represent himself in the proceedings or have other comparable representation in his place. The Court held that there was a violation of Article 6 § 1 of the ECHR, reiterating that the principles of equality of arms and adversarial proceedings are key elements in the concept of a fair hearing. Parties before the court must have a "reasonable opportunity of being heard with adequate knowledge of the submissions and evidence put before the Court." In this instance, the Court reasoned that Vasilyev's personal testimony describing the conditions of his treatment in custody were indispensable, first-hand knowledge that constituted a key part of his argument. Given his lack of opportunity to testify during the proceedings, the Court held that there was an Article 6 violation.
See https://www.globalhealthrights.org/vladimir-vasilyev-v-russia/

Gorbunov and Gorbachev v. Russia, 1 March 2016 *(An individual must be able to follow proceedings).*
In Gorbunov and Gorbachev, the Court held that proceedings against the applicants were unfair due to insufficient arrangements having been made to ensure effective legal assistance during the appeal hearings. Concerns existed with regards to: the quality of the video link provided to the accused and thus the ability to follow proceedings; the contact between the applicants and their lawyers (video link versus in person); and constraints on that lawyer-client relationship in terms of trust and understanding (due to temporal and logistical issues with privacy).

Trepashkin v. Russia (no. 2), 16 December 2010 *(There must be opportunity for private communication between a defendant and their lawyer).*
In Trepashkin, the Court found no violation of Article 6, but it underscored the importance of confidential communication between defendants and their lawyers. The accused should be able to confer with lawyers out of the hearing of third parties, exchange notes and documents freely with their lawyers, and have access to case files. Another factor to consider is the conditions in which the accused is transported and confined to the courthouse, specifically whether it affects the accused's ability to prepare properly for hearings.

According to the Consultative Council of European Judges (CCJE), information technology (IT) should be a tool or means to improve the administration of justice, to facilitate the user's access to the courts, and to reinforce the safeguards laid down in Article 6 of the ECHR.[23] In Opinion No. 14 of the CCJE (Strasbourg 7-9 November 2011),[24] they recommend that:

- 'Judges must … eliminate any risks to the proper administration of justice. IT must not diminish parties' procedural rights. Judges must be mindful of such risks as they are responsible for ensuring that parties' rights are protected' (Article 7).

- 'The use of IT should not diminish procedural safeguards for those who do not have access to new technologies. States must ensure that parties without such access are provided specific assistance in this field' (Article 10).

- 'The use of IT should not, however, diminish the procedural safeguards (or affect the composition of the tribunal) and should in no event deprive the user of his/her rights to an adversarial hearing before a judge, the production of original evidence, to have witnesses or experts heard and to present any material or submission that he/she considers useful. Moreover, the use of IT should not prejudice mandatory hearings and the completion of other essential formalities prescribed by the law. You must also retain, at all times, the power to order the appearance of the parties, to require the production of documents in their original form and the hearing of witnesses. Security requirements must not be an obstacle to these possibilities' (Article 28).

- 'Video-conferencing may facilitate hearings in conditions of improved security or the hearing remotely of witnesses or experts. It could, however, have the disadvantage of providing a less direct or accurate perception by you of the words and reactions of a party, a witness or an expert. Special care should be taken so that video-conferencing and adducing evidence by such means should never impair the guarantees of the defence' (Article 30).

- 'The role of IT should remain confined to substituting and simplifying procedural steps leading to an individualised decision of a case on the merits. IT cannot replace the judge's role in hearing and weighing the factual evidence in the case, determining the applicable law and taking a decision with no restrictions other than those prescribed by law' (Article 31).

[23] Consultative Council of European Judges, Opinion No.14 of the CCJE *Justice and information technologies (IT)*, Adopted by the CCJE at its 12th plenary meeting (Strasbourg, 7-9 November 2011), https://rm.coe.int/168074816b, para 5.

[24] Consultative Council of European Judges, Opinion No.14 of the CCJE *Justice and information technologies (IT)*, Adopted by the CCJE at its 12th plenary meeting (Strasbourg, 7-9 November 2011), https://rm.coe.int/168074816b.

- ‘Judges should be involved in all decisions concerning the set up and development of IT in the judicial system;
- Consideration must be given to the needs of those individuals who are not able to use IT facilities;
- Judges must retain, at all times, the power to order the appearance of the parties, to require the production of documents in their original form and the hearing of witnesses;
- IT should not interfere with the powers of the judge and jeopardise the fundamental principles enshrined in the Convention.’[25]

You should be alert to the need to ensure that the defendant and other participants make full use of all the safeguards to which they are entitled. Some research has shown that those appearing before the court remotely may be less likely to ask for legal representation because they could consider the process less legitimate or serious.[26]

[25] Ibid, section F.

[26] Ingrid V. Eagly, *Remote Adjudication in Immigration,* 109 Nw. U. L. Rev. 933 (2015), https://scholarlycommons.law.northwestern.edu/nulr/vol109/iss4/2; Fielding, N., Braun, S. and Hieke, G. (2020). *Video Enabled Justice Evaluation.* Sussex Police and Crime Commissioner and University of Surrey, https://www.sussex-pcc.gov.uk/media/4862/vej-final-report-ver-12.pdf

C. National legal framework

A national legal framework for conducting hearings remotely provides essential guidance for the court and the participants. Where there is no legal provision for remote proceedings in national law, it may still be feasible to hold them depending on the other procedural standards and regulations in place. As a judge you should:

- Rely on your national legislation when deciding whether to hold a hearing remotely or in person. The court should not organise a remote hearing if the legislation forbids it.
- Read the national legislation carefully to ensure that a remote hearing will not be contrary to any provision of the law.
- Look to any guidelines or other published advice from national higher judicial authorities (e.g., judicial councils), which have recently been drafted and released in many jurisdictions, setting out how to conduct remote hearings and proceedings.
- Look to tools that may have also been developed by local lawyers and bar associations. For example, the Council of Bars and Law Societies of Europe (CCBE) has also formulated Guidance on the use of remote working tools by lawyers and remote court proceedings.[27]

[27] CCBE, *Guidance on the use of remote working tools by lawyers and remote court proceedings,* 27 November 2020, https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20201127_CCBE-Guidance-on-the-use-of-remote-working-tools-by-lawyers-and-remote-court-proceedings.pdf

CHAPTER 3:
DETERMINING WHETHER A MATTER IS SUITABLE FOR REMOTE PROCEEDINGS

Checklist

General factors should be considered such as:

- ✓ The complexity of the evidence
- ✓ Whether the parties consent
- ✓ If the individual is in detention
- ✓ Time limits
- ✓ If the defendant has legal representation
- ✓ Length of the hearing
- ✓ Authentication of documents
- ✓ Whether the hearing needs to be in public
- ✓ The circumstances of the participants
- ✓ Cost
- ✓ Vulnerabilities

Evidentiary issues:

- ✓ How to manage evidence
- ✓ Whether parties have access to scanned versions of evidence
- ✓ Whether the court IT platform has an option for uploading evidence
- ✓ Use of official email of the court for correspondence

Special considerations for cases which raise particular challenges:

- ✓ Children and juveniles

- ✓ Disabilities of the parties
- ✓ Sexual violence and domestic abuse cases
- ✓ Language interpretation or other special support is required
- ✓ Where examination of physical evidence is crucial

Technical limitations:

- ✓ Seek information about participants' technical capacities
- ✓ Whether the participants have access to the necessary technologies and, if not, whether alternatives can be found
- ✓ Whether confidential communication will be possible
- ✓ The suitability of the court's internet connection
- ✓ The availability of a camera and microphone in the courtroom
- ✓ Consider holding the hearing in segments to avoid lengthy screen-time

It is for you, as the judge, to ultimately determine whether a particular proceeding is suitable to be held remotely.

A. General factors

There are a number of factors which may assist you:

- Undisputed cases, cases of procedural agreement, and pre-trial hearings may be more suitable for remote proceedings than first appearance hearings, particularly in criminal cases;
- Whether the parties consent;
- Whether the individual is in detention;
    - Can the detention facility provide adequate internet connections?
    - Will the use of remote hearings expedite the case?
- Whether there are time limits by which the case needs to be heard (e.g., considerations of speedy resolution and the need to hold the hearing within a reasonable time);
- The number of participants, which may also affect the duration of the hearing and provide additional technical challenges;
- Whether the parties have legal representation;
- The length of the hearing (e.g., if it is a preliminary hearing lasting less than an hour);
    - In bankruptcy or pre-bankruptcy proceedings, you might want to divide the creditors in groups and have a remote hearing separately for each group when possible. This will enable you to gain more control over the entire hearing and avoid cases where large numbers of creditors are on the screen at the same time.
- Is authentication of documents and identity possible, e.g., through electronic signature;
- Where the evidence is undisputed or is not complex, it may be more suitable for remote proceedings. For example:
    - Less complicated civil cases, such as small claims proceedings
    - Non-contradictory matters

    - Commercial cases with request for payment where the facts of the case are clear and where there is no need to take additional evidence, just paper documents

- How will public participation be facilitated;

- Are there particular circumstances of the participants that favour or require holding the hearing remotely? (e.g., they are in another country, the cost of travel, health issues, childcare, physical safety and security, or other reasons meaning they are unable to attend court);

- Are there vulnerabilities and disabilities of the participants, and will this limit their ability to participate fully, either in-person or online.

B. Evidentiary issues

The nature of the evidence may also be a factor in determining suitability:

- When deciding to hear a case remotely, be aware that you will need to manage how to receive, send, and examine evidence, motions, and decisions remotely.
- Will it be sufficient if the parties have scanned versions of evidence and examine them by sharing the screen with all participants (for example, where the evidence is documentary only and the originals are in the custody of the court).
- Check if the IT platform used by your court has an option for uploading evidence by the parties and if the parties can see their own and each others' files remotely.
- If there are no other options, consider using the official email of the court for exchanging documents with parties.

C. Special considerations

The following cases may raise particular challenges for remote hearings:

- Cases involving children or juveniles;
- Certain criminal law matters;
- Particular disabilities of parties;
- Sexual and domestic violence cases;
- Cases in which language interpretation or other forms of special support and assistance are required;
- Cases where examination of physical evidence by the judge and by expert witnesses is crucial.

D. Technical limitations

When considering the suitability of cases for remote judging, you should keep in mind the technological capabilities of the court, parties, attorneys, and other participants. It is essential to ascertain the following information in advance of the hearing:

- What are the technical capacities of the parties?
- Do participants have access to the necessary technology to enable their full participation (e.g., appropriate bandwidth, audio and visual equipment, etc.)?
- If the participants lack the necessary technology, can alternatives be found—such as using the offices of lawyers, notaries, or other public officials?
- Will the participants be able to communicate in confidence with their legal representatives during the course of the remote hearing?
- What is the internet infrastructure in the court, and does it sustain the platform you want to use (check that with your IT court advisor)?
- Does the courtroom you are going to use for the remote hearing have a proper camera and microphone that will allow you to be heard and seen by participants without constant disruptions?
- Can the hearings be divided into reasonable time segments to reduce the time spent on screen?

E. Cross border issues

In considering a remote hearing in cross border matters, Council Regulation (EC) 1206/2001 applies. The purpose should be to facilitate the presence and participation of the parties, their legal representatives in taking evidence, and enable the actual presentation of evidence.

A connection needs to be established between the courtroom in the state where the hearing will take place (requesting court), and the courtroom or other location in the foreign state where the evidence is presented (requested state). The parties, their legal representatives and the judge may be located in one (domestic) state and other parties, legal representatives or/ and witness/es will be in another (foreign) state. It may be possible to hear a witness without first getting permission from the other country, when the witness is not in court.

- Before a remote hearing of witness/expert witness/party in a foreign state, you should check if witness/expert witness/party can be heard online by the judge of another state, with or without the approval of the competent authority of the foreign state.

- Bilateral/multilateral and/or other agreement/s, if applicable, will need to be checked.

In a request for a remote (court) hearing by video link or online hearing, it is necessary to inform the requested (foreign) state in detail and to suggest a technical way in which such international legal assistance would be provided. Any further communication regarding the mutual submission of the necessary data and deadlines should take place through the competent authority (e.g. Ministry of Justice).

The following principles should apply:

- According to Council Regulation 1206/2001, requests for videoconference or teleconference should be complied with unless incompatible with the laws of the requested state.

- The establishment of video links depend on the approval of the requested authority and on the availability of equipment and technical support. Permission to use a video link can be requested. It is recommended that before the official submission of the request, the authority of the requested foreign state be contacted in order to confirm whether the use of a video link is possible.

- Requests should specify the video link requirements, such as: whether additional assistance is needed; the equipment or facilities are available and / or required (e.g. to facilitate the transfer of image documents between two locations in real time), together with relevant technical details, as appropriate for witnesses/ experts/others.

Establishing a video connection may be contrary to the domestic law of the other state, could be impossible to enforce it because of its own internal practice and procedure, or there may be difficulties of a practical nature. In such cases, if the parties and/or witness give testimony from their home or other premises then the judge from domestic state shall examine the parties and/or witness/es in accordance with the procedure and the law of the state in which the proceeding is taking place.

1. Time and place

- The court determines the time and place of the remote hearing, indicating the relevant conditions for the video link, taking into consideration time differences and other specific conditions.
- If the premises of the foreign / requested court or authority are being used, then the time and place of the remote hearing shall be determined in consultation/ agreement between the courts/authorities.
- It should be noted/specified in the request/summon whether the legal representatives who are in the domestic / requesting state wish to cross-examine the witness / expert via video link in the foreign / requested state.
- Some jurisdictions do not allow cross-examination by representatives of the other state, although this may be allowed if the lawyer from the domestic state is authorized to practice law in the territory of the foreign state.

2. „Direct“ taking of evidence

- Before the start of the hearing, the judge should:
- Check the location of the witness/expert.
- Ensure that the witness/expert is willing to testify via video link/remotely.
- Determine how to establish identity of party/witness / expert.

3. „Indirect“ presentation of evidence

Where evidence is to be delivered or presented from a foreign country, the court of that country shall conduct an inquiry (adhering to the manner and procedure in accordance with the national law of that foreign state).

4. Language and interpretation

- Evidence must be presented in, or translated into, the language in which it can be executed, namely the language of the court of the requesting state.

- If interpretation is required for a witness or expert, the organizers of the hearing by video link should take into account the qualifications and experience of the interpreter in particular in the context of the use of video link technology and the conduct of remote hearings.

- Some jurisdictions have a system for the registration of qualified or sworn interpreters and translators.

- *Consecutive interpretation* is usually used and it is preferable if the interpreter and the witness or expert are located in two different locations, as this facilitates clarification or intervention.

- *Simultaneous interpretation*, which is more demanding, requires an interpreter‘s booth and special equipment, and may require multiple interpreters.

- The location of the interpreter whose services will be used for the remote hearing should be taken into account in advance - whether the interpreter will be at a remote location where the witness is located or at the main, domestic location.

5. Costs

- Consideration needs to be given to costs, including the possibility of seeking relevant forms from the foreign / requested authority in order to reclaim costs.

- The foreign court authority in the requested state, if necessary, may claim reimbursement of the costs incurred in using the video link, including transfer fees, equipment rental and technical support fees, fees for the use of video link equipment, communication fees (eg for the use of the Internet or telephone connection), fees for technicians and external video service providers, i nterpretation fees, and court costs (e.g. payment of overtime when the hearing via video link is held outside regular working hours). Some courts may have fixed costs.

CHAPTER 4:
TECHNOLOGIES AND CASE MANAGEMENT

Checklist

When considering the use of different IT platforms, ask questions about:

- ✓ Ease of use and reliability
- ✓ The image of the court on the screen
- ✓ Safety and security of the platform(s)
- ✓ Tools to control proceedings, including muting and unmuting participants
- ✓ Equal opportunities for all parties to participate, including through chat function
- ✓ Accommodation and accessibility to persons with disabilities
- ✓ Ability to facilitate private lawyer and client communication
- ✓ Opportunities to switch from a real to a virtual courtroom
- ✓ Does it provide the ability to record proceedings
- ✓ Whether recordings can be paused
- ✓ Where records of digital proceedings or recordings are saved
- ✓ The required server capacity
- ✓ How participants are invited
- ✓ The capacity to schedule hearings using the IT platform
- ✓ Can the platform support or accommodate provision of transcription services
- ✓ Can the platform accommodate translation and interpretation services
- ✓ The possibility of enabling live streaming or a web feed for relevant proceedings.

A. Different technological platforms

There are currently a large range of viable software platforms in use by courts across the CEE region. These include: Cisco's Webex, Zoom, JITSI, Google Meet, Microsoft Teams, Skype, Polycom Real Presence, BlueJeans, PEXIP, and TrueConf, as well as bespoke platforms for particular courts. In considering a platform for remote proceedings, judges should review whether they:

- Are easy to use;
- Are reliable;
- Are able to provide an appropriate image of the judge, the courtroom, and the participants on the computer screen;
- Are considered sufficiently safe from security breaches;
- Provide specific tools so that the judge can control the procedures and prevent misuse;
- Provide each party equal opportunities to participate;
- Enable you and the parties to have control when questioning a witness.

When comparing platforms, it may also be helpful to consider the following:

- Whether it provides you with similar, or more, ways of managing the process than a non-remote hearing;
- What is the server capacity needed to function effectively;
- What are the features for recording sessions;
- Whether an independent file is created after each pause, for example, or whether the program allows for the recording to be paused and continued;
- Where the records are saved (on the local computer or in the cloud);
- How participants are invited (e.g., by email);
- Whether there is the capacity to mute and unmute individual participants;
- Whether there is a chat function;

- The timeframe in which a hearing can be scheduled (e.g., a minimum/maximum time in advance);
- How accessible it is to persons with disabilities (e.g., visually impaired, deaf, mental capacities, etc.) or other vulnerabilities;
- How are transcription, translation, and interpretation services provided for;
- Whether the platform can provide live streaming or a web feed in proceedings that are deemed public, and whether it has facilities for relaying this to the media.

B. Case management

Digital case management, where available, serves as an efficient way of logging the files, storing evidence, and exchanging necessary written data between participants and the court. Some of these systems allow participants to not only communicate remotely, but also ensure a high level of security and enable authentication of documents, case allocation, as well as scheduling of hearings.

In some jurisdictions, files may be kept both in paper form and electronically; in others, the formal file may be kept only in paper. You should be aware of data being lost if electronic evidence is converted into paper form. Specifically, the 'metadata' that electronic files also include, which is electronic information about other electronic data, might be lost if files are converted to paper format. For example, the electronic data also contains information such as the author and date of creation or any revisions. If the court is only provided with printouts of electronic data (e.g., email), then some of this metadata will be lost.

C. Hybrid hearings

One option available to many courts is to schedule a 'hybrid' hearing, where some of the participants will be in the courtroom and others will join the hearing remotely. Various factors should be considered:

- You should ensure that the advantages and disadvantages of in-person and remote participation are explained and understood by the parties and that the decision is made with fully informed consent, in order to uphold the principle of equality of arms.

- Consider that hybrid hearings present new kinds of potential technical problems, particularly with regard to microphones and camera placement. Discuss the nature of the planned hybrid hearing with your IT support personnel, in advance, if possible.

- All participants, whether present in person or joining remotely, should be able to participate fully and equally in the proceedings. This can be managed by the court continuously verifying the connection—the ability of the participants to hear, speak, and see everything.

- If a remote participant is a witness, you should consider the authenticity, reliability, and credibility of the witness as well as the absence of influence from other individuals.

CHAPTER 5:
PRACTICAL TIPS FOR MANAGING REMOTE HEARINGS

Checklist

- ✓ Preparation is key to successful remote hearings.
- ✓ Advance training on use of the relevant IT platform is obligatory.
- ✓ The decorum and authority of the courtroom must be upheld in online settings through the use of formal language, dress, and adapted rituals and by managing disruptive participants.
- ✓ The court should ensure a safe and secure environment for all participants.
- ✓ Public access, where required by law, must be ensured.

Questions to ask when preparing for a remote hearing:

- ✓ Is a remote hearing suitable for the specific case, bearing in mind the legal framework and subject of the case?
- ✓ Has consent of the parties been obtained?
- ✓ Has consideration been given to the needs of participants with vulnerabilities and disabilities?
- ✓ Which type of remote proceeding is more suitable – 'hybrid hearing' or remote hearing?
- ✓ What preparations can be made in advance of the hearing?

Questions to ask during a remote hearing:

- ✓ What are your options for checking the identity of the remote participants?
- ✓ When and how will you explain the rules and the process of the hearing and the technical issues?
- ✓ How will you ensure that the participants conduct themselves appropriately during the hearing?

- ✓ How will you explain and apply the rules for disruptive participants?
- ✓ How can private lawyer-client communication be ensured?
- ✓ How can undue interference on remote witnesses be prevented?
- ✓ How will you deliver the judgment?
- ✓ How will you ensure that the hearing is public?

A. Preparing for a remote hearing

1. Initial Considerations

In order to ensure the hearing is conducting appropriately, you (and court staff) must prepare in advance.

- Determining the knowledge and experience of participants with using remote technology may help avoid challenges during the hearing. Some participants may have little knowledge of the software or other technical issues presented in a remote hearing, and they may not understand how to participate. Providing information (and training, if necessary) in advance of the hearing can avoid problems on the day of the hearing itself.

- It is strongly advised that the participants, whenever possible, join remote hearings using a stable internet connection via LAN/Ethernet internet instead of WiFi connections. The court should so advise participants in advance of the hearing

- Test equipment and software platforms in advance of the hearing; become familiar with how to use the selected platform and ensure others are also familiar.

- The court must ensure enough time is provided for the remote hearing.

- You should be confident using the technology and equipment needed for the remote hearing. However, technical difficulties will occur and should be expected. If possible, you should have an IT specialist available to help manage technical problems during the hearing.

- Before the start of the hearing, all technical requirements must be checked and tested, including test calls to ensure everyone has a good connection.

- You should also prepare yourself physically and psychologically given the impact that prolonged on-screen concentration can have on your health.

2. Issuing guidance in advance

Guidance should be provided to participants before the hearing on the preferred conduct, obligations, and procedures during the hearing. This guidance should be available on the website of the court, along with some tutorial videos.

- Have an assistant or a secretary collect the emails of participants in order to then send them an invitation to the hearing. If a participant does not have an email, they could be asked to create one.

- Consider whether the rules will be the same for remote hearings as for in-person hearings and how those rules will be applied in remote hearings.

- When preparing for the hearing, the court should send in advance (by e-mail or other legal service) the guidance, rules on behaviour, and relevant warnings or cautions to the parties. Remind the parties the need to have official ID available for verification. An electronic link to the remote hearing could also be sent at this stage.

- In situations where the court is sending a subpoena or other order to the parties setting the hearing date, the court should send to participants the electronic order or subpoena with the same information as in non-remote cases. It is essential to draft such an order or subpoena in a manner that makes it clear that the hearing will be remote.

- Ideally court staff, rather than you as the judge, should ensure proper preparation in advance of any remote hearing. This should include court staff:

    - Checking if participants have the necessary technical capacities to join the hearing.

    - Sending participants information on how to use the platform and any contact information if there are technical questions or other problems with accessing the remote hearing.

    - Sending forms in advance via email (e.g., oath) and login details for the hearing, as appropriate.

    - Offering to test connections with participants in advance of the hearing, including a test call on the day of the hearing.

    - Requesting that all participants call in/log on a short time before the hearing is due to start.

- Confirm that the link to the software platform is correct and operable.

- The judge and the participants must be properly dressed, according to the dress code and customs of that court. This is particularly important to clarify in advance of the hearing given that some of the participants may be joining the hearing from their homes. If someone is not dressed appropriately, you should intervene and seek a change. The court must inform participants of the rules in advance.

- It is prudent to ask participants for their consent for participation in a remote hearing, even if that is not required by the law.

- At the commencement of the remote hearing, you should make sure that all present have received and understood the guidance and that they are aware of their obligations, restrictions, and the manner of conduct. You should review the rules at the start of the hearing, explaining clearly and in detail how the hearing will be conducted and the consequences of disruption.

- Consider how to handle the following contingencies in advance of the hearing:

    - How warnings will be given.

    - Use of the 'mute' function to stop interruptions or disruptive or inappropriate behavior (e.g., using 'mute all' can avoid potential challenges that one participant will feel unfairly excluded).

    - Determine in advance under what circumstances it may become necessary to exclude or remove a party from a hearing and how this will be achieved with the particular platform.

    - How to adjourn or postpone hearings.

    - How to make and save necessary recording or transcription of the hearing

    - How to enter a note in the record or transcript of the hearing, setting out what has happened.

    - Ensure that participants are familiar with all relevant rules.

- You should be aware of the circumstances of the participants and their physical location, including whether they are participating from outside the country. In cases where parties are participating from another jurisdiction, the court must confirm in advance whether the software program and procedures used for the remote hearing can be used in the other jurisdiction.

- Cases involving domestic violence or sexual abuse will require particularly sensitive handling. If the hearing is in private (e.g., in family cases, domestic violence cases, or sexual abuses cases), the parties should be on their own, unless you give them permission for someone else to be with them. For example, in cases with child witnesses or victims, the presence of a parent, psychologist, or social worker may be required. If necessary, you should consider whether, given the challenges that may arise, the hearing should be held only in-person.

- Depending on the location from where the individual is giving testimony, guidance could be provided which asks participants to consider:

- Lighting;
- Background;
- Sound; and
- Angle and positioning of the camera (to ensure it is able to capture the whole room, as well as the gestures, facial expressions of the participant, etc.).

3. Scheduling hearings

- When scheduling a hearing, you should be aware of whether parties are joining from different time zones or different jurisdictions.
- Ensure more time than for an in-person hearing, keeping in mind, for example, technical difficulties, delays, the need to explain the procedure, having to repeat statements in case of poor connection, etc.
- More frequent breaks may be required; research has noted the psychological impact of 'Zoom fatigue.'[28]
- Consider having participants provide a scanned ID in advance of the hearing.
- As necessary, provisions should be made for the necessary technology and equipment to be provided to participants who will not otherwise have remote access. This includes proper accommodation of those with disabilities, similar to accommodations and adjustments which would normally have been made to them for in-person hearings held at court.

4. Keeping a written record of the hearing

Producing a written record or minutes from a remote hearing may pose particular issues in terms of how to produce, sign, and reduce [it/them] to written form:

- If the national law requires, the hearing should be recorded.
- Consider whether to record the video hearings in those instances where national law and regulations permit recording the hearing (or are silent on the matter).
- Where required, the court should produce a record or minutes of the proceedings and send it via email to the participants to check and sign it, electronically, if possible.

[28] Bailenson, J. N. (2021). *Nonverbal Overload: A Theoretical Argument for the Causes of Zoom Fatigue. Technology, Mind, and Behavior*, 2(1), https://doi.org/10.1037/tmb0000030

- The entire remote justice procedure should be carefully and fully outlined and explained in the court hearing transcript – including information about the platform used for videoconferencing, the physical location of the remote participants, explanations about the procedural rules being used, and warnings provided to the participants.

- In cases where the hearing is recorded, attention should also be given to requirements under laws ensuring personal data protection and privacy, such as the the General Data Protection Regulation (GDPR). You should consider whether portions of the hearing should not be recorded, for example, when the identities of the participants are checked or they discuss personal information. This may be particularly important in cases where the hearing is broadcast live or may be re-broadcast.

- Consider the technical requirements if you should need to periodically pause, silence, or hide participants from the camera at moments during the hearing.

5. Being aware of unconscious bias

You should be aware of unconscious bias if individuals are giving testimony by video link. For instance, some research has shown that children giving evidence by video link can be perceived as less credible because their demeanour cannot be fully assessed or because jurors question why they are giving evidence remotely.[29]

6. Being aware of the impact on your well-being

Remote judging can impact on your psychological and physical well-being. Remote hearings can be more demanding than in-person hearings and may result in feelings of being isolated and disconnected.

[29] Goodman, G. S., Tobey, A. E., Batterman-Faunce, J. M., Orcutt, H., Thomas, S., Shapiro, C., & Sachsenmaier, T. (1998). *Face-to-face confrontation: Effects of closed-circuit technology on children's eyewitness testimony and jurors' decisions.* Law and Human Behavior, 22(2), 165–203. https://doi.org/10.1023/A:1025742119977; Antrobus, E., McKimmie, B.M., and Newcombe, P. (2016). *Mode of children's testimony and the effect of assumptions about credibility.* Psychiatry, Psychology and Law, 23:6, 922-940, pp.3 DOI: 10.1080/13218719.2016.1152927

B. Identification of parties

There are various ways of verifying participants' identities:

- By showing an ID or passport to the camera. If there are doubts or there is no clear view of the document, the proceeding should not continue until this is resolved. For purposes of privacy, this segment of the hearing should not be broadcast online or recorded.

- By requesting the participants to send to the court a scanned copy of their ID cards or passports in advance of the hearing. This can then be compared to the IDs shown on camera at the beginning of the hearing, allowing the court to compare and confirm the relevant versions.

- By previous registration with the relevant ID. The participant could be registered online, by use of electronic signature, through a national database or other digital platform. When identity is confirmed, the hearing can proceed.

- By confirmation at the office of a notary/lawyer or other authority. The participant could attend the remote hearing from the office of a public notary, lawyer, or other authority. This solution provides both confirmation of identity and a secure environment for the participant to participate in proceedings.

- By identification by police. The police could identify the participant in their home, for example, at the start of the remote hearing.

- By recognition by parties or witnesses. If there is no other way of identification at the court's disposal, other participants, if possible, could identify the individual and confirm their identity. False statements are punishable by law.

C. Principles of conduct during remote proceedings

You have the responsibility to manage the court, ensure compliance with court rules, and ensure that there is appropriate decorum. This will require vigilance and patience during the proceedings. International and national standards of fair hearings, including the Bangalore Principles,[30] should be used as the benchmark against which to uphold the authority of the court.

Recommendations for national authorities, Councils of Justice, Judicial Associations, and other competent authorities:

- All authorities, such as Judicial Councils, Ministries of Justice, Judicial Academies, etc., have a responsibility to prepare judges and participants for remote judging.
- Manuals from competent judicial authorities on how to conduct remote hearings should be developed and widely shared with judges (e.g., through podcasts, videos on their sites, and other promotions).
- Such manuals should be provided to the participants with the notice of hearing and be available on the court website.

1. At the start of the hearing:

- Remote hearings should be clerked, and the clerk should manage the admission of the parties before you are admitted into the virtual court room.
- The judge should, at the outset of the remote hearing, set out what the various processes will be (e.g., mute/video and other facilities, introducing who is in court, and how to raise questions).
- Explain how technical difficulties will be handled.
- Assure the parties that all legal requirements are met and that the remote hearing will be full and fair.
- When appropriate, and in line with the rules for that court, explain that the hearing will be digitally recorded, but that the participants may not make their own recordings.
- Explain the consequences for disrupting proceedings.
- Allow participants the opportunity to ask questions about these matters.

[30] Bangalore Principles of Judicial Conduct, adopted by the Judicial Integrity Group in 2001, as revised at the Round Table Meeting of Chief Justices in The Hague, Netherlands, on 25-26 November 2002, https://www.unodc.org/pdf/crime/corruption/judicial_group/Bangalore_principles.pdf

- At this stage, you should consider postponing the hearing if the participants do not have the necessary technology in place to ensure their full participation

2. Decorum

- The decorum of the remote hearing is an important element in guaranteeing the court's authority.

- Court insignia should be visible. The digital platform should consider where the judge is positioned on the screen and how other participants are aligned and arranged, according to their role in the process.

- Proper lighting and background also play important roles in creating the professional and serious atmosphere necessary to uphold the authority of the court and for it to be able conduct the hearing smoothly.

- Use of formal language and phrases, as well titles of the parties, is obligatory for all the participants.

- Ensure that participants comply with the usual rules of court etiquette and good practice, including:

    - How to address the judge and one another.

    - The processes for asking to speak.

    - The rules regarding the format and sequence of the particular hearing.

    - Consequences for disruptive participants; conveying understanding, if necessary, that disruptive participants will be muted.

- Recognize that a remote hearing may take longer and require additional comfort breaks. Breaks should be sufficiently frequent (e.g., five to fifteen minutes every 60-90 minutes) to avoid visual impairment and pain. Participants should be permitted to move during the break periods (leave the room or building).

- Monitor the participants throughout the proceeding to ensure they are participating fully (e.g., checking if the screen has frozen, etc.) and react quickly and appropriately if there are problems. You may need to repeat what has just occurred if a participant was unable to follow the proceedings.

- You should draw upon other court staff, including IT specialists if available, to ensure the smooth running of the remote hearing.

3. Managing disruptive participants and consequences and penalties for disruption

It is the duty of you as the judge to maintain and ensure order during the hearing. This includes sanctioning disruptive action by any participant. International and national standards on fair hearings should be maintained in managing disruptive participants. If there are no specific rules for remote hearings, then the same rules with respect to in-person hearings should apply.

- Parties should be reminded, in those jurisdictions where it is applicable, that it is an offence for a person to make or attempt to make an unauthorized recording or transmission of court proceedings – which includes images. Thus, it is unlawful to take photographs or videos of a hearing conducted remotely.
- Parties should also be reminded that giving a false statement is a crime.
- A disclaimer on the screen during the remote hearing could also assist in providing a constant reminder to all participants.
- You should monitor the participation and behaviour of participants during the hearing to ensure their full attention and engagement.
- Warn participants of problematic behaviour.
- 'Mute' participants as necessary.
- Pause or adjourn the hearing.
- Subject to national law and policies, remove the disruptive participant from the hearing if their presence is not compulsory.
- Subject to the laws and rules of your jurisdiction, impose a fine or other procedural discipline.

4. At the end of the hearing:

- Confirm that all parties have been able to follow the proceedings.
- Provide the judgment, if appropriate, or, if not, inform the parties when they might receive it.

D. Communication between client and lawyer

Communication between a party and their lawyer is a guaranteed right. It may be facilitated in various ways during remote hearings. It is necessary to identify software platforms for hearings that can provide appropriate mechanisms and functions to facilitate such private and privileged communication. Examples include:

- **'Break-out rooms'** – some platforms provide for separate break-out rooms which could be used for private and secured communication between two or more users.

- **'Private Chat' option** – some platforms provide for a separate, secure private chat option that may be used for counsel-client communication during the hearing.

- **'Leave a party alone.'** The court could announce a short break requiring other participants to leave the platform for a set period of time.

- Suggesting that the lawyer and their client **mute themselves** so they remain in the hearing but cannot be heard.

- Use of **other private channels**. The court should allow participants to communicate via other applications, or phone, as long as there are no restrictions by law (for example, the participant might communicate with her attorney via WhatsApp, while the hearing itself is conducted on Zoom)

E. Remote testimony

1. General considerations

You must remain vigilant, active, and sensitive to the needs and challenges of parties and witnesses giving testimony remotely. In particular, you must be alert to any vulnerability. Given some of the challenges with assessing the credibility of a witness remotely, you may wish to consider whether sworn written testimony can be used more extensively.

Witnesses and parties giving remote testimony need to be treated with dignity and respect.

2. Preparation

- Consider having a pre-trial hearing to verify the practical and logistical capabilities of the court and participants.

3. Location

- Testimony should be given from neutral and secure locations.
- The court may consider providing rooms in the courthouse from which witnesses can give their testimony. Such rooms could have a computer that has the necessary IT to enable their participation in the hearing.
- Where the court has concerns about potential interference with the testimony, the court may direct that the individual give testimony from a location that is officially registered, such as another courthouse, an appropriate state agency, the offices of lawyers for the relevant parties, or mediators' offices.
- If the accused is to give testimony from custody or prison, the background, their clothing and any information on the screen should not identify the location if this will impact on their presumption of innocence.
- Where individuals are giving testimony from a private location, such as their home, they should provide the address to the court.

4. Support for witnesses

- The court should have the support infrastructure in place for remote proceedings, e.g. a special room for examination of witnesses, a family room, educational equipment and other materials for family or children.
- Witnesses should be provided with additional support by professionals (or guardians) where appropriate.

- Witnesses should be provided with a court-registered interpreter if they do not speak the language which is the official language of the court. This may require special software platforms or special online accommodations. Do not underestimate the technical challenges of conducting a remote hearing in more than one language; the technical challenges are significant and not all platforms are suitable. These considerations must be worked out in advance and should be done at the expense of the court.

5. Support for and managing witnesses with vulnerabilities

Particular attention, at an early stage, should be paid to considering the vulnerability of participants, even if you are not alerted to such by the parties. Vulnerability can be assessed through a range of factors which may limit the individuals' ability to participate in the case. These may be evident through, for example, their age, maturity and understanding; mental or physical capacity; social and cultural background and ethnic origins; their domestic circumstances and religious beliefs; demeanour and language; the circumstances of the alleged offence; other characteristics; the information before the court; or the questions being put to them.

6. Preventing and managing undue interference

As part of the right to a fair hearing and the principle of equality of arms, witnesses must not be subject to undue influence or interference. You should:

- Consider what the witness can see compared to the image that you can see.
- Ask the witness to position themselves on the screen so you are able to see their gestures.
- Ask the witness to make a statement at the start of their testimony that they are not being subject to any undue interference and that there is no one in the room with them.
- In the case of vulnerable witnesses, including minors, the court should consider having persons present with the witness who can offer professional support for the witness.
- For proceedings involving minors, exclude the possibility of interference from a parent to the child, particularly when the child is a victim of sexual abuse. You could also consider excluding any parent or guardian who is interested in the outcome of the proceeding.
- Consider utilizing the services of notaries, where available, to:
    - Enable witnesses to provide their statement in writing duly executed.

- Provide office space and the necessary technical equipment for them to participate in a remote hearing.

- Verify the identity of the witness and then confirm this before the court, prior to testimony being taken by the court.

- Ask the witness to 'show' you around the room in which they sit by holding and rotating the camera on their device. This procedure could be repeated throughout the hearing as necessary.

- Ask the witness to give testimony from a room with only one door and then ensure the camera is focused on that door during the proceedings. You can then call on any person entering the room to leave immediately.

- Ask the witness to sit away from the screen so as to avoid them reading any material from the computer. If there is a concern that the witness has been reading from a prepared script, consider asking them questions to ascertain if this is the case.

- Where permitted, provide a confidential chat facility, mobile phone number, or other electronic device to permit the witness to engage directly with you if they have concerns.

- Utilize separate 'rooms' on the platform in which witnesses can wait before you permit them to 'enter' the hearing.

- Explain how witnesses and other participants may attract your attention during the hearing (e.g., through hand gestures, using the 'chat' function, asking you questions directly, etc.).

- If several witnesses in the same location are to be questioned remotely, there is a risk that witnesses may communicate with each other. This risk may present additional logistical challenges that vary with the relevant physical layout. Such risks can be minimized in various ways; for example, the court may choose a larger room with enough empty chairs where those who have given their testimony can then sit, visible to the court, until all witnesses have been questioned.

- Take into account all of these issues and the risk of undue interference in assessing the credibility of the witness.

7. When should the court interrupt or stop the testimony of a witness?

- If there are technical challenges, such as if the connection is poor.

- If the witness is under duress.

- If there are insufficient guarantees of a secure environment for the witness.
- If the court is not able to identify the witness and there is no positive recognition, then the testimony should be adjourned until identification is completed.

F. Public access

- Consider both legal requirements and technical options for opening a hearing to the public.
- Will the hearing be accessible to all or only to pre-registered participants or those authorized to attend? If so, how will the latter be managed (e.g., through password protected log-ins, etc.)?
- Will pre-registration for the hearing be required? Hearings could be streamed online to a wider public audience or to a smaller number of attendees who have previously registered and subscribed.
- Instruct observers, including the general public and media, at the outset of the hearing that unauthorised recordings or transmission of the hearing is illegal. Further advise on the consequences of such action.
- In some situations, a recorded broadcast could be made available, following the live hearing, on the court's website or video channel sites (e.g., YouTube).
- Media representatives could help facilitate online access to a hearing.
- A secure link from one room in the court house for journalists to follow the hearing could also be considered.

CHAPTER 6:
DATA SECURITY, PRIVACY, AND STORAGE

Checklist

- ✓ Remote hearings should adhere to the standards of the GDPR and/or any other domestic laws and regulations on protection of data and privacy.
- ✓ Privacy and security are integral to data integrity and can be ensured through using encrypted cloud-based platforms, providing a back-up system, and creating a list of participants in advance.
- ✓ You should be aware of the locations of participants in a remote hearing.
- ✓ Consider file-sharing via a conference or cloud storage platform and the challenges posed by email.
- ✓ It is for ultimately for the court to determine the probative value of evidence received remotely or through digital means.

To authenticate and store documents securely:

- ✓ Copies of messages or emails should include the electronic timestamps, showing the date and time of each message as well as the contact information of the sender.
- ✓ All documents received by the court, if not already in PDF format, should be converted and locked in PDF format to prevent subsequent editing or tampering.
- ✓ Access to evidence shared and stored digitally should be controlled and access points limited.
- ✓ The court must name each evidentiary submission and exhibit clearly and ensure they are easy to locate.

A. Introduction

The Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence[31] provide a number of fundamental principles to keep in mind when managing electronic evidence:

- 'It is for courts to decide on the potential probative value of electronic evidence in accordance with national law.'[32]
- '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.'
- 'It is also necessary to ask what the legal basis is for submission of evidence electronically.'
- 'The General Data Protection Regulation (GDPR) applies in the EU and is based on seven principles: Lawfulness, Fairness, and Transparency; Purpose limitation; Data minimisation; Accuracy; Storage limitation; Integrity and Confidentiality (security); and Accountability.'
- 'You should be aware of the issues relating to electronic evidence, but it is for the parties to submit data in a secure manner to the court.'

Furthermore, under the principle of equality of arms, the Guidelines also state:

- '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.'[33]

---

31 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), CM(2018)169-add1final: https://rm.coe.int/guidelines-on-electronic-evidence-and-explanatory-memorandum/1680968ab5

32 See also, European Court of Human Rights, *García Ruiz v. Spain,* No. 30544/96, paragraph 28.

33 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), CM(2018)169-add1final: https://rm.coe.int/guidelines-on-electronic-evidence-and-explanatory-memorandum/1680968ab5

As the Committee of Ministers Guidelines explain:

- ‘Electronic evidence should be neither discriminated against nor privileged over other types of evidence.’

- ‘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.’

The GDPR and domestic laws on protection of data and privacy will apply to remote hearings and communications in judicial proceedings within the EU, and the processing of personal data outside the EU may be subject to data protection regimes equivalent to that of the GDPR.

B. Types of documentary evidence

Documentary evidence includes email, photos, videos, etc. in both hard and soft copies. The most common types of evidence shared in remote hearings are: documents, emails, videos, and text messages. For physical evidence (weapons, etc.), items can be photographed or videotaped and those images then made available via screen sharing.

- The court must allow for digital evidence to be submitted electronically. The court must, as necessary, guide the parties through the process and provide technical conditions for sharing and use of such evidence.

- As the judge, you must at all times hold the evidence on electronic devices maintained by you or the court.

C. Privacy and confidentiality issues

Privacy and security are integral to data integrity, and data integrity is crucial for a fair hearing. Privacy can be ensured by the following:

- Courts should use encrypted, cloud-based video conferencing.
- As has been noted above, it is strongly advised that the participants, whenever possible, join remote hearings using a stable internet connection via LAN/ Ethernet internet, instead of WiFi connections. The court should so advise participants in advance of the hearing.
- While conducting the remote hearing, the court should always provide a back-up system for each hearing and assign an IT specialist to monitor the electronic compliance of the system and provide technical support.
- A list of participants, their full names, professional affiliation, and details of the locations from which they will be joining the hearing should be agreed and circulated to the parties in advance. Where the hearing is public and/or will be covered by the media, the participants should be so advised in advance.
- You or the IT controller must only allow individuals on the approved or preregistered list of participants to join the remote hearing, subject to prearranged conditions regarding the public nature of the hearing
- There should be the possibility for separate virtual break-out rooms. These should be password protected.

There is a need to ensure that the right to privacy is protected when the hearing is public. As a judge it is your responsibility to use the various tools and ensure this balance is met:

- Learn the platforms. Familiarize yourself with the settings and properties of the common platforms as well as the protection of the privacy of the participants and the attending public.
- Those wishing to attend a hearing who are members of the public, including the media, could request the judge for participation.
- If the trial is of high public importance and it is open to the public, you should always require additional technical safeguards to verify the identity of all authorized participants who require virtual access.
- As a judge, you are responsible for broadcasting the proceedings. It is paramount to communicate the proceedings to the public and the media in advance to promote compliance and prevent unauthorized disruptions of proceedings or the improper use of court footage.

- If YouTube is used to broadcast the hearing, then a warning should be made at the start of the hearing that it will contain personal data.
- Participation for the public and media could be granted through a secure link.
- Even if the trial is public, you should always consult the local witness exclusion orders, so that witnesses who have yet to be heard are not influenced by prior testimony.

Privacy threats can be divided into several categories:

1. Unauthorized access to evidence

The unauthorized access to evidence in remote hearings and the sharing of digital evidence risks intrusion of privacy and can jeopardize the entire judicial process.

2. Location

You must be aware of the location of the parties and witnesses in remote hearings. The location may present security and privacy concerns, especially in cases of domestic violence. Some jurisdictions require witnesses to swear under oath that no one else is present or listening. As noted above, techniques such as asking witnesses to pan around the room to demonstrate that no one else is present can be used to limit such interference.

3. File-sharing

File-sharing via the conferencing platform or a cloud storage platform is more secure than using e-mail. However:

- You must always consider the sensitivity of the information, the type of hearing involved, and the level of security required.
- Email is widely accessible, but it may not be a particularly secure method of transmission for sensitive information. Emails can contain errors, such as the wrong subject line, failing to attach the intended file, or attaching a completely unrelated file. The date sent and received can result in confusion over which is the most current version. Additionally, in terms of security, emails are the common entry points for destructive viruses and malware.[34]

[34] Federal Bureau of Investigation. 2021. *CJIS Security Policy Resource Center.* [online] Available at: https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

D. Authenticating documents and ensuring data security

Data manipulation and alteration pose significant risks to the integrity of evidence. Electronic evidence can be modified to change the date, time, and content. Good evidence handling practices are important to ensure that digital evidence is protected from both intentional and unintentional modification.[35]

- Evidence should be submitted in its original form.
- The party relying on the evidence should be able to provide detail of its authenticity, such as through metadata and from trust providers.
- Courts should always consider the reliability of the evidence, including its source.
- Screenshots of messages are useful and include identifying information linking the message to the sender. A testimony or affidavit that the copy is a true and accurate representation of the text messages can serve as authentication.
- Where possible, copies of text messages or emails should include the electronic timestamps showing the date and time of each message as well as the contact information of the sender (phone number and/or email address).[36]
- To prevent modification, all documents should be converted and locked in PDF format.
- Notarization of documents is an often-used method for providing authenticity of court documents and statements submitted by the parties. They can, however, be costly in terms of time and money.

National legislation and rules will set out what is required in terms of authenticating documents. Examples include:

- That the document be submitted electronically and accompanied by a letter;
- That the document be submitted with an electronic signature.

E-signatures

It is essential for the conduct of remote court proceedings that documents are provided to the court through technological and electronic means. The flexibility of remote judging will be enhanced if court administrations are able to ensure that judges and staff can sign certain

---

[35] UNODC. 2021. *Cybercrime Module 6 Key Issues: Handling of Digital Evidence.* [online] Available at: https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/handling-of-digital-evidence.html

[36] *Text Messages as Evidence: A How-To Overview.* MassLegalServices, 24 October 2019, https://www.masslegalservices.org/content/text-messages-evidence-how-overview

documents electronically. Judges and court staff should have an understanding of electronic signatures in order to be able to deal with issues such as the identification, authenticity and credibility of an electronic document.

The courts should also consider the use of electronic signatures as a mean for providing authentication of documents when presenting evidence.[37] The eIDAS regulation[38] provides a framework for electronic signatures and authentication services.[39]

An electronic signature is "any type of signature in electronic format".[40] eIDAS[41] defines 'electronic signature' as a "data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign".[42]

Provided it complies with the relevant regulations,[43] an electronic signature will have the same status as a handwritten signature, and signify the individual's intention to be bound.[44]

The eIDAS Regulation[45] defines three levels of electronic signature:

- ‚simple' electronic signature,
- advanced electronic signature and
- qualified electronic signature.

---

37 Autenti. 2021. *What methods can be used to authenticate people who place an electronic signature?* [online] Available at: https://autenti.com/en/blog/what-methods-can-be-used-to-authenticate-people-who-place-an--electronic-signature

38 European Commission. 2021. *Shaping Europe's digital future: eIDAS Regulation.* [online] Available at: https://digital--strategy.ec.europa.eu/en/policies/eidas-regulation; Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, https://eur-lex.europa.eu/eli/reg/2014/910/oj. The regulation on electronic identification and trust services for electronic transactions in the internal market is also known as the "eIDAS Regulation."

39 For further guidance see https://rm.coe.int/cepej-2021-15-en-e-filing-guidelines-digitalisation-courts/1680a4cf87; https://www.coe.int/en/web/cdcj/activities/digital-evidence; https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&qid=1645791279459&from=EN; and https://matsne.gov.ge/ka/document/view/3654557?publication=1
https://signify.ge/legal

40 Cryptomathic (2021.), *What is an electronic signature?* [online]. Available at: https://www.cryptomathic.com/products/authentication-signing/digital-signatures-faqs/what-is-an-electronic-signature

41 Regulation (EU) No 910/2014 Of The European Parliament And Of The Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

42 eIDAS, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&from=EN#d1e791-73-1

43 eIDAS in the European Union: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&from=EN#d1e791-73-1; NIST-DSS y САД-y, https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf; and ZertES in Switzerland, Understanding ZertES - the Swiss Federal Law on Electronic Signatures, https://www.cryptomathic.com/news-events/blog/understanding-zertes-the-swiss-federal-law-on-electronic-signatures

44 What is an electronic signature?,
https://ec.europa.eu/digital-building-blocks/wikis/display/CEFDIGITAL/What+is+eSignature

45 eIDAS, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&from=EN#d1e791-73-1

Simple Electronic Signatures – can include writing your name in an email.[46]

Advanced Electronic Signatures (AdES), according to Article 26 of eIDAS is an electronic signature that:

> ‘(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 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’.[47]

A public-key infrastructure (PKI) is the most used technology, employing certificates and cryptographic keys.[48]

Qualified Electronic Signatures (QES) is defined by Article 3 of eIDAS as “an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures”.[49] Signature creation devices are defined as “configured software or hardware used to create an electronic signature” and can include smartcards, SIM cards, USB sticks. „Remote signature creation devices“ can also be used if the person signing does have not physical possession of device.[50]

46 What is an electronic signature?, https://ec.europa.eu/digital-building-blocks/wikis/display/CEFDIGITAL/What+is+eSignature

47 eIDAS, Article 26, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&from=EN#d1e791-73-1

48 What is an electronic signature?, https://ec.europa.eu/digital-building-blocks/wikis/display/CEFDIGITAL/What+is+eSignature

49 eIDAS, Article 3, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&from=EN#d1e791-73-1

50 What is an electronic signature?, https://ec.europa.eu/digital-building-blocks/wikis/display/CEFDIGITAL/What+is+eSignature

E. Sharing and storage

Access to evidence shared and stored digitally should be controlled and access points limited. Electronic audit logging should document when files are accessed and by whom. The Committee of Ministers Guidelines[51] provide helpful guidance on storage and preservation and archiving data:

- 'Electronic evidence should be stored in a manner that preserves readability, accessibility, integrity, authenticity, reliability, and, where applicable, confidentiality and privacy.'[52]
- It should be stored in its "original format" (i.e., not as printouts) and in line with relevant laws.[53]
- 'The readability and accessibility of stored electronic evidence should be guaranteed over time, taking into account the evolution of information technology.'[54]
- 'The integrity of electronic evidence should be maintained at all stages.'[55]
- '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.'[56]

51 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), CM(2018)169-add1final: https://rm.coe.int/guidelines-on-electronic-evidence-and-explanatory-memorandum/1680968ab5

52 Ibid, Guidelines: "Storage and preservation", sec. 25, p. 11.

53 Ibid, Explanatory Memorandum Guidelines: "Storage and preservation," sec. 44, p. 26.

54 Ibid, Guidelines: "Storage and preservation," sec. 27, p. 11.

55 Ibid, Explanatory Memorandum Guidelines: "Storage and preservation, sec. 46, p. 27.

56 Ibid, Guidelines: "Archiving," sec. 28, p. 11.

This project was made possible by a grant and ongoing support from the U.S. Department of State's Bureau of International Narcotics and Law Enforcement Affairs (INL)

CEELI Institute
Villa Grébovka
Havlíčkovy Sady 58
120 00 Prague
Czech Republic

www.ceeliinstitute.org
office@ceeli.eu