

CM-Public

MINISTERS' DEPUTIES

CM Documents

CM(2021)36-add5-final

16 June 2021

1407th meeting, 16 June 2021

10 Legal questions

10.1 European Committee on Legal Co-operation (CDCJ)

Guidelines of the Committee of Ministers of the Council of Europe on online dispute resolution mechanisms in civil and administrative court proceedings - Explanatory Memorandum

CONTENTS

GENERAL COMMENTS.....

PREAMBLE

PURPOSE AND SCOPE

DEFINITIONS

FUNDAMENTAL PRINCIPLES

THE GUIDELINES

APPENDIX CYBERSECURITY CHECKLIST FOR MEMBER STATES

BIBLIOGRAPHY

GENERAL COMMENTS

Why a new instrument?

1. Online dispute resolution (ODR) techniques and mechanisms play an increasingly important role in dispute resolution in the Council of Europe member States. ODR has the ability to improve access to justice by facilitating faster and less costly access to courts, thereby making dispute resolution more effective and efficient.
2. However, wide use of ODR also has the potential to restrict access to justice by setting up technological barriers to all those who do not have the capacity to use technology. Moreover, attention needs to be given to issues of authentication and identification of the parties, digital divide, cybersecurity and personal data protection.
3. To ensure that disputes are resolved fairly, there is a need to develop appropriate and adequate guidelines on human rights protection in the use of ODR. Within the member States of the Council of Europe, this requirement also follows from the guarantees enshrined in the Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 5 the "European Convention on Human Rights"), especially the judicial guarantees contained in Articles 6 and 13. To date, there are few such standards at international, European, and at national levels. These guidelines aim to recommend standards to shape law and practice and fill existing gaps.
4. These guidelines suggest a set of baseline measures that member States' governments, legislators, courts as well as ODR developers, manufacturers and service providers should follow in order to ensure that ODR do not undermine human dignity, human rights and fundamental freedoms.
5. The purpose of these guidelines is not to establish binding legal standards but rather to serve as a practical tool for member States to ensure that their ODR techniques and mechanisms comply with the requirements of Articles 6 and 13 of the European Convention on Human Rights and the principles developed in the jurisprudence of the European Court of Human Rights in respect of those articles. The guidelines do not impose any obligation on member States to introduce ODR into their national law or to enlarge the use of ODR.

Working method and the drafting process

6. The issue of ODR falls within the competence of the European Committee on Legal Co-operation (CDCJ) which is the Council of Europe's intergovernmental body responsible for standard-setting activities in the field of civil and administrative law.
7. In 2016 a study was undertaken on the feasibility for the CDCJ to undertake an activity on ODR mechanisms with reference to Articles 6 and 13 of the European Convention on Human Rights.
8. As a follow-up to this, the CDCJ decided to start, in 2017, work on the preparation of a technical study as a first step of the activity. This technical study has been completed and presented to the CDCJ at its 93rd plenary meeting (14-16 November 2018).
9. The activity was continued with the preparation of these guidelines aiming at ensuring the compatibility of ODR mechanisms with Articles 6 and 13 of the European Convention on Human Rights. The guidelines are based on the proposals made by CDCJ members and were prepared at the meetings held in 2019 and 2020. The drafting group took into consideration experience arising from the operation of ODR mechanisms in place in member States.

National examples:

- In **Lithuania** online filing, online payment of court fees and digital cases materials with online access are available in all civil and administrative cases using the centralised e-justice system LITEKO; courts normally issue digital official documents (orders, decisions, judgments, rulings, notifications, summons, etc.) authenticated by qualified electronic signatures and having the same legal value as analogous paper documents; in 2019 about 74 percent of court case files in civil and administrative matters were digital, other files were mixed (digital and physical/paper); property sale auctions in enforcement

proceedings are held only electronically; videoconferencing can be used in civil and administrative procedures as almost each court is equipped with at least one set of video-conference equipment or may use mobile video conferencing equipment and every court room is equipped with equipment for digital audio recording. As a response to Covid-19 outbreak all judges of the Lithuanian courts were provided with the possibility to work from their homes with remote access to justice system LITEKO. Steps were taken to start more active use of video and teleconferencing with widespread private tools (such as videoconferencing) for conversion of oral hearings into virtual digital meetings. Additional cybersecurity measures were implemented to ensure safety and stability of the e-justice system.

- In **France**, it is possible to initiate administrative and commercial proceedings online on dedicated portals and to submit court documents in an electronic way. It is possible to use videoconferencing in civil proceedings.
- In **Greece**, all procedural acts (i.e. claim, appeal, remedy etc.) and the documents that support them (written statements with attached files as evidence) can be filed electronically by the lawyers with the use of a qualified electronic signature. Videoconference during the main proceedings is also permitted.
- **Ireland** has an online court platform for certain small claims. As well as this, the following services are also available: an online eLicensing system to process licensing applications including alcohol related licences and gaming and lottery applications etc., the Legal Costs Adjudication system which allows claims to be made online, the Court Fines Online system which allows for electronic payment of fines imposed by the District Court, and the Supreme Court online system which allows for application for leave to appeal to the Supreme Court to be made online. Additional measures have also been introduced to provide for remote hearings in civil proceedings, the electronic submission of documents to courts in advance of proceedings known as "eFiling", the remote submission of "Statements of Truth" as an alternative to sworn affidavits, and for bodies conducting hearings or appeals to do so via remote means.
- In **Poland** the procedure for payment orders is fully electronic. The claim is submitted through an individual account created on a dedicated IT platform. All acts and documents are available online.
- In **Portugal** eviction proceedings, meant to enforce the termination of lease contracts, can be initiated over an online platform ("Balcão Nacional de Arrendamento"). Citius is an e-platform used by courts. Legal representatives can use it to submit their procedural documents and notifications. Also in administrative and tax jurisdictions, via SITAF online system, legal representatives can submit their procedural documents, be notified and consult their cases electronically. Both systems (Citius and SITAF) also support the activities of magistrates and public prosecutors. Parties to the proceedings have online access to documents relating to their cases. Certificates concerning court proceedings can also be obtained electronically. All national courts are equipped with at least one video conference room and all courtrooms have audio recording systems.
- **Belgium** introduced the Central Solvency Register ("RegSol"), a digital platform enabling creditors, authorised agents and interested parties to commence, access or follow up pending insolvency files administered by the Business court.
- **The United Kingdom** introduced: 1) a MONEYCLAIMS platform online and 2) an ODR platform to resolve cases resulting from airline passengers.
- In **Hungary** artificial intelligence is used in the online anonymous judgment database (searchable records).
- **Turkey** has implemented the National Judiciary Informatics System called "UYAP", enabling courts and individuals to carry out procedural acts online.

10. The present guidelines take full account of the Committee of Ministers 2019 Guidelines on electronic evidence in civil and administrative proceedings (hereinafter the "guidelines on electronic evidence").

Structure and content

11. The present guidelines largely follow the structure of principles developed in the jurisprudence of the European Court of Human Rights under Article 6 of the European Convention on Human Rights as helpfully compiled in the Court's "Guide on Article 6 of the European Convention on Human Rights – Right to a fair trial (civil limb)".

12. While in these guidelines the conditional "should" is frequently used, where the relevant principles are taken from the European Convention on Human Rights and case-law of the European Court of Human Rights the use of the conditional "should" must not be understood as reducing the legal effect of the European Convention on Human Rights.

PREAMBLE

13. The present guidelines apply to ODR used in court proceedings concerning civil (including commercial) and administrative disputes, be it a compulsory or voluntary instrument (for the definition of "court", see paragraph 18 below). The diversity of legal systems of member States is fully acknowledged and the guidelines are intended to be general enough to accommodate all the different legal systems. In particular, the guidelines do not provide any recommendations to member States as to whether they should introduce ODR techniques and mechanisms in their judicial systems. On the other hand, the guidelines are not only a declaration of principles but aspire to give practical advice and guidance.

PURPOSE AND SCOPE

14. The present guidelines address, in particular, the key principles of a fair trial and effective remedy as interpreted by the European Court of Human Rights in its case-law, for example, the principle of equality of arms.

15. The guidelines aim to assist member States in ensuring that ODR techniques and mechanisms are compatible with Articles 6 and 13 of the European Convention on Human Rights without compromising the benefits which ODR can bring, in particular, in so far as the costs of dispute resolution are concerned. In this context, it should be reiterated that the provisions of the European Convention on Human Rights must be interpreted in the light of present-day conditions, while taking into account the prevalent economic and social conditions (*Marckx v. Belgium*, 13 June 1979, §41, Series A no. 31; *Tyler v. the United Kingdom*, 25 April 1978, §31, Series A no. 26).

Key provisions of the European Convention on Human Rights

Case-law of the Court on Article 6(1) provides: "In the determination of his civil rights and obligations (...) everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interests of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice."

Case-law of the Court on Article 13 provides: "Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity."

The guidelines deal with:

fair procedure;
transparency in the use of ODR and requirements for hearings;
special issues related to the ICT nature of ODR techniques;
other issues (not stemming from the jurisprudence of the European Court of Human Rights).

16. There is a widespread confusion regarding the use of the term "ODR". It is frequently understood as the electronic variant of the alternative dispute resolution (ADR), typically organised outside the court. An example is the European Union Online Dispute Resolution Platform. However, these guidelines concern use of new technologies in existing in-court proceedings. The reason for this is the focus of these guidelines: they deal with the question of how the guarantees referring to court procedures contained in Articles 6 and 13 of the European Convention on Human Rights can be secured when electronic mechanisms for resolving disputes are being used, in other words what legal and technical conditions these mechanisms must fulfil in order to meet the requirements stemming from Articles 6 and 13 of the European Convention on Human rights. Out-of-court and non-court-related dispute resolution, i.e. "alternative dispute resolution (ADR) mechanisms, do not fall under Articles 6 and 13 and therefore are intentionally excluded from the scope of these guidelines. However, member States may decide to extend the implementation of these guidelines to ADR, such as arbitration or mediation, accordingly if and where appropriate. While doing so, member States should be aware that the guidelines were drafted and aligned to existing in-court proceedings. This means that not all of the particular guidelines can be directly applied and may need to be further adjusted by member States to be used *mutatis mutandis* within specific ADR mechanisms.

17. The guidelines do not apply to internal management of electronic case files by the courts. This includes, for example, the algorithm for allocation of cases among the judges.

DEFINITIONS

Court

18. A broad definition of "court" is included in order to cover all authorities with competences to adjudicate legal disputes using ODR in civil and administrative proceedings. Direct reference is made to the concept of a "tribunal" in the meaning of Article 6 of the European Convention on Human Rights in order to align the scope of these guidelines with the scope of Article 6. In its judgments the European Court of Human Rights set out the criteria for the court to be recognised as tribunal in the meaning of Article 6 of the European Convention on Human Rights and those criteria are fully reflected in the guidelines. The guidelines cover proceedings before bodies entrusted with decision making functions and only those proceedings which are of a judicial nature. This delimitation is important because other activities carried out by such bodies may be of non-judicial nature. These guidelines do not apply to non-contentious and unilateral procedures which do not involve opposing parties and which are available where there is no dispute over rights (*Alaverdyan v. Armenia*, application no. 4523/04, decision on admissibility of 24 August 2010, § 35; *Cyprus v. Turkey* [GC], no. 25781/94, ECHR 2001-IV).

Online dispute resolution (ODR)

19. The term "online dispute resolution (ODR)" first appeared in the late 1990s and has developed over two decades in line with the expansion of the Internet and, particularly, online shopping and other transactions. Initially, the concept was associated only with alternative dispute resolution (ADR) mechanisms that used electronic communications, which is especially convenient in cases where the parties are located far away from each other. ODR was and is still widely used as a synonym of electronic alternative dispute resolution (eADR). For example, Regulation No 524/2013 of the European Parliament and of the Council, of 21 May 2013, limits its scope to the "out-of-court resolution of disputes concerning contractual obligations stemming from online sales or service contracts between a consumer resident in the Union and a trader established in the Union". However, it should be noted that over the years the meaning of the term "ODR" has been extended to comprise also techniques and mechanisms that complete, speed up and facilitate many functions of the traditional courts.

20. It may sometimes be difficult to differentiate the concept of ODR from other related but different concepts, such as, the concept of "cyberjustice". The latter refers to the general incorporation of technology into the justice system. According to the "Guidelines on how to drive change towards Cyberjustice" (CEPEJ, December 2016), Cyberjustice is "broadly understood as grouping together all the situations in which the application of ICTs, at least, forms part of a dispute resolution process, whether in or out of court". Consequently, the concept of Cyberjustice is broader than that of ODR, encompassing ODR mechanisms, but also others.

21. For the purposes of these guidelines, ODR refers to technology used for dispute resolution that is carried out remotely through the use of computers, including mobile devices, and the internet. ODR is not in itself a form of dispute resolution but rather refers to information technology (IT) that is used in the existing in-court proceedings. This is not a new type of proceedings and not an alternative to any such in-court proceedings. ODR provides new ways of access to the existing types of in-court proceedings. The concept follows from the ongoing transformation of national judicial systems into more digitalised form with remote access for the parties. ODR mechanisms are designed to facilitate electronic communications and in order to obtain an outcome without the need for the physical presentation of documents or for physical presence at a court meeting or hearing. In this line, United Nations Commission on International Trade Law (UNCITRAL) Technical Notes on Online dispute resolution, New York 2017, define ODR as a "mechanism for resolving disputes through the use of electronic communications and other information and communication technology".

22. The guidelines cover such ODR techniques as:

- i. online filing systems/platforms directly accessible for the parties and/or their representatives for the filing of statements (such as claims, counterclaims, responses, etc.);
- ii. online systems for storing, processing and assessing electronic evidence;
- iii. artificial intelligence, big data analysis techniques and automation, to the extent that they affect court proceedings;

- iv. platforms for online court meetings and online hearings, for example by audio- and videoconferencing, including giving of oral testimony by witnesses and experts.

Artificial intelligence (AI)

23. Artificial intelligence (AI) is a broad and rapidly evolving area of information and communication technology (ICT) that enables automated reasoning. It creates the potential for making automated decisions, recommendations and forecasts and thus can make civil and administrative proceedings more effective, accessible and affordable.
24. However, it is important to understand that ODR is not the same as AI. Not all ODR mechanisms involve AI components. ODR is a wider concept covering all kinds of online mechanisms for dispute resolution, including tools for automation that do not necessarily include an element of AI. The distinction between ODR and AI is kept throughout the guidelines. While the requirements to meet the guarantees stemming from Articles 6 and 13 of the European Convention on Human Rights apply to all ODR mechanisms, regardless of whether they involve AI elements or not, certain questions in this context bear increased significance with regard to AI mechanisms. This is particularly true for questions referring to automated decision-making without human intervention and the possibility for reviewing those decisions.
25. An AI system is an information system operating in the form of software or integrated in a physical hardware device that solves complex problems and functions in both physical and digital dimensions. Such a system functions by perceiving its environment through the collection and interpretation of collected, structured and unstructured data, drawing conclusions from available knowledge, processing information obtained on the basis of this data in order to make decisions on the most appropriate action to be taken in order to achieve the desired goal.
26. For the purposes of these guidelines, the definition of AI is that proposed by the European Ethical Charter on the use of artificial intelligence in judicial systems and their environment adopted by the European Commission for the Efficiency of Justice (CEPEJ) on 3-4 December 2018. The Charter sets out five principles which guide the development of AI tools in the European judicial systems. Those five principles are reflected in the guidelines dedicated to AI. The present guidelines also take into consideration the definition of AI proposed in the European Commission Communication on AI, as further elaborated by the Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission. The guidelines also follow the definition of AI system included in the Recommendation of the OECD Council on Artificial Intelligence adopted in 2019.

Information and communication Technology (ICT)

27. "ICT" means "Information and communication Technology" and refers to technology that provides access to information through telecommunications. This includes the Internet, wireless networks, cell phones, and other communication media. For example, ODR users can communicate in real-time using technologies such as instant messaging, voice over IP (VoIP), and videoconferencing.

FUNDAMENTAL PRINCIPLES

Principle 1

28. Building trust and confidence in ODR is crucial for the proper use of ICT in the courts. It is now frequently the case that people, sometimes even judges, have doubts regarding use of ODR mechanisms, in particular where AI components are involved. The main challenge is how member States can build and enhance trust and confidence in ODR. This can be done only by applying the same key principles of a fair trial and effective remedy as interpreted by the European Court of Human Rights in its case-law in the context of existing in-court proceedings. These basic principles need to be further explained and transposed into the ICT context. The particular challenges arising from the application of these principles in the ODR context need to be analysed and addressed.

29. These guidelines can be used by member States to create a sound legal and ethical framework for using ODR. A human rights approach should constitute the starting point in designing the ODR mechanisms to make justice effective and efficient. Member States may also build and enhance trust and confidence in ODR by explaining to the public that use of ODR is not meant to fully replace the existing in-court proceedings but rather to supplement them and create additional options for access to justice. ODR needs to be seen as an ancillary aid to judicial decision-making, and to facilitate the judge's work, not as a constraint. ODR has to be adapted to the needs of judges and other users, and it should never infringe guarantees and procedural rights such as that of a fair hearing before a judge. ODR should improve the administration of justice, facilitate the user's access to the courts and reinforce the safeguards laid down in Article 6 of the European Convention on Human Rights: access to justice, impartiality, independence of the judge, fairness and reasonable length of proceedings.

Case-law of the Court of Justice of the European Union

The judicial protection mentioned resulting from Articles 6 and 13 of the European Convention on Human Rights is assured as long as electronic means are not the sole means for accessing the (settlement) procedure (Joined Cases C-317/08 to C-320/08, Rosalba Alassini and Filomena Califano v. Wind SpA, Lucia Anna Giorgia Iacono v. Telecom Italia SpA and Multiservice Srl v. Telecom Italia SpA, ECJ judgment of 8 March 2010, paras. 58 and 60).

Principle 2

30. ODR can contribute to more effective and efficient access to justice. However, the main obstacle to much wider use of ODR is access to technology. Some people do not have the necessary skills or facilities to use ODR and have a dispute resolved online (the "digital divide"). For example, they may be unfamiliar with using digital applications or may not have access to Internet, a computer or other tools or technologies. This group of people should be able to benefit from an appropriate assistance. Member States should develop ODR in such a way that the digital divide is adequately addressed. For example, ODR mechanisms can be kept optional.

Authorities can set up support kiosks in court buildings or in legal aid bureaus. Supportive programs for the public can be created. The use of pilot schemes and user-feedback also help to address the digital divide problem. As it is explained in the guidelines, ODR mechanisms should have a simple and user-friendly interface to enable as many people as possible to use the technology.

Principle 3

31. The principle requires that where no particularities stem from the specific use of ODR mechanisms, procedural issues should be subject to the same rules that apply to the respective court procedure generally. ODR can and should be subject to the same due process standards that apply to the court procedure in an offline context, in particular independence, neutrality and impartiality. Any adjustments to the general procedural rules introduced due to the specific nature of an ODR mechanism must not undermine the principles of fair trial and effective remedy.

Principle 4

32. It is important that the parties to proceedings involving ODR are properly identified and there is no identity fraud. Separation of the digital identity from the physical one may generate problems related to the identification of the parties. In the first place, courts should seek to establish the identity of the parties. Such secure mechanisms include, in particular: i) certificates to electronic signatures, sometimes referred to as the "digital ID" of a person; ii) confirmation of identity by a payment system operator that has been used for paying court fees online; iii) public trust services providing technological mechanisms that ensure proper identification.

THE GUIDELINES

Fair procedure*Access to justice*

Guideline 1

33. Justice is for everyone. In many member States applicants can lodge their cases without being represented by a lawyer, therefore it is particularly important to make the whole process easily understandable for its users. In order to enhance accessibility, the design of ODR should keep user interfaces as simple and intuitive as possible. If possible, the ODR instruments should be made accessible 24/24, 7/7 and from different computer and mobile devices operating systems. ODR should allow parties to use standard forms, upload related documents and receive timely responses. By means of ODR courts may also use real time communication. As far as a national legal system permits, technical tools available in ODR can offer flexibility regarding the language used in the proceeding, for example, by built-in translation programs, in case of multilingual proceedings involving parties from different countries or cultures. The principle of user-friendliness is not to be understood as being limited to litigants and their representatives but ODR tools should be equally user-friendly to judges and other court staff.

Guideline 2

34. Parties need access to all the necessary information. It is important then that appropriate assistance, information and feedback is provided to users. The design of ODR can make assistance (for example, tutorials) easily available to users. This includes information on how to submit a claim and receive information about the progress of the case. ODR may structure the process itself for litigants. It also means that dispute resolution through ODR can be done almost anywhere, making the process convenient and easy for litigants.

European Court of Human Rights' case-law

When the relevant law provides individuals with a possibility of lodging a complaint without being represented by a lawyer, domestic courts should advise applicants on how to remedy the formal deficiencies of their complaints (*Wende and Kukówka v. Poland*, no. 56026/00, § 54, 10 May 2007).

Magna Carta of Judges

The "Magna Carta of Judges" adopted by the Consultative Council of European Judges (CCJE) in 2010 emphasised in paragraph 14 on "access to justice and transparency" that "justice shall be transparent and information shall be published on the operation of the judicial system".

National example: Poland

In Poland applicants are provided with the possibility to find all relevant information on necessary formal requirements and technical issues on the e-court's website (general information on the e-court, information for applicant, for defendant, examples of correct and incorrect applications, FAQs, regulations on online payments, etc.).

Guideline 3

35. Essentially, each party must be given a fair and equal opportunity to argue his or her case as to both matters of fact and law and each party should have a right to react to and rebut the submissions of the other party. Evidence and relevant material must be disclosed to both parties in an accessible and adequate way. ODR speeds up processes, but also risks increasing information overload (which slows down information processing). Because of that, while disputes should be dealt within a reasonable time, parties should be granted reasonable time periods for reaction.

European Court of Human Rights' case-law

The principle of the equality of arms implies that each party must be afforded a reasonable opportunity to present his case – including his evidence – under conditions that do not place him at a substantial disadvantage vis-à-vis his opponent (*Letinčić v. Croatia*, no. 7183/11, § 48, 3 May 2016).

Guideline 4

36. ODR design needs to be guided by the internationally recognised technical standards, such as Design for All principles in the ICT context. This implies user-centred approach and that the use of ODR should not be hindered by the existence of barriers in their technical design and functionalities, nor by the inherent cost of their use. Following these standards will make content accessible to a wider range of people, such as persons with disabilities and make ODR more accessible to users in

general. In particular ODR implementation may not be limited exclusively to text communication but allow and enable parties' visual and audio communication (video or audio conferences). Development of ODR systems allowing for more efficient types of communication should be promoted. This does not preclude designing of ODR systems which provide multiple choice communication types (text, audio, visual or various ICT). ODR should function properly to ensure confidentiality of communication, enabling the contact which is unfettered by any practical or other obstacle (*Marcello Viola v. Italy*, no. 45106/04, § 63-77, CEDH 2006-XI (extracts); *Golubeva v. Russia*, no. 1062/03, 17 December 2009).

Guideline 5

37. ODR has the potential to create cost savings by its very nature and to provide an economical alternative to proceedings handled in the traditional way. As a consequence, it is reasonable to expect that the cost of ODR use for the parties should be at least neutral in relation to the costs of access to the justice system using on-site resources. When general principles of exemption from costs and free assistance exist, they should be applicable to ODR.

Guideline 6

38. Parties should be notified when it is intended that their case will be processed with an ODR tool that involves an AI mechanism. In particular litigants have a right to obtain information on the reasoning underlying AI data processing operations applied to them. This should include the consequences of such reasoning. This transparency requirement is also confirmed by all existing recommendations, ethical codes and guidelines establishing ethical standards for designing, deployment and use of artificial intelligence, as established by the Council of Europe, the United Nations bodies, European Union, OECD and other international institutions. These standards need to be respected by designers, engineers, providers, administrators and professional users of ODR.

Equality of arms

Guideline 7

39. The guideline makes it clear that ODR should not deprive a party of the right to be heard by the court. The rights of access to a court, to adversarial proceedings and to an effective judicial remedy are fundamental rights of individuals that are safeguarded under the European Convention on Human Rights. While important, the objectives of achieving efficiency and expediting proceedings cannot justify infringing these rights.

Guideline 8

40. Independence and impartiality in ODR decision-making processes are essential requirements in order to ensure compliance with standards of the European Convention on Human Rights. Trust and confidence in ODR are built by avoiding the existence of - or any perception of - bias towards the interests of any of the parties. Article 6(1) of the European Convention on Human Rights explicitly states that the court must be independent and impartial. It is even more important for ODR as they may entail a process where the adjudicator is not physically present and trust issues may arise as a consequence.

Guideline 9

41. Knowledge of, and access to, the materials in the case-file, including those submitted by other parties is an essential requirement for fair proceedings. Moreover, the materials in the case-file, including all relevant metadata, should be sufficiently precise and detailed to enable the parties to challenge or contest their contents if they wish to do so. Where the time is insufficient for a party, a possibility to request an additional time should be available. The guideline covers not only access to documents submitted by the other parties, but also to the materials in the case-file, which often includes documentation produced by the court itself.

European Court of Human Rights' case-law

The requirement of "adversarial" proceedings under Article 6 of the European Convention on Human Rights entails having an opportunity to know and comment on the observations filed or evidence adduced by the other party. "Adversarial" essentially means that the relevant material or evidence is made available to both parties (*Ruiz-Mateos v. Spain*, 23 June 1993, § 63, Series A no. 2).

Evidence

Guideline 10

42. It is important to ensure that parties to proceedings involving ODR are not placed in a disadvantageous position because of their lack of access to digital services or their lack of understanding of how the services operate. ODR should be as user-friendly as possible and not operate in a manner that would be likely to prejudice the interests of any of the parties. See the guidelines on electronic evidence for further reference (in particular, in the part concerning fundamental principles).

Guideline 11

43. The use of electronic evidence may create specific challenges for a party wishing to challenge the authenticity or integrity of such evidence. ODR should provide appropriate safeguards in order to facilitate such a challenge. Instructions, templates or other tools can be used for this purpose. For example, where a party challenges the electronic evidence, the party seeking to rely on the evidence may be required to demonstrate its authenticity, for example by submitting metadata or seeking an appropriate order to obtain additional data from other persons, such as trust services providers. The reliability of electronic data may be proved in any manner, for example, by qualified electronic signatures or other similar methods of identification and ensuring integrity of the data. Provisions of national legislation establishing the evidential value of public (official) electronic systems that generate electronic evidence should be respected. Moreover, parties should be permitted to challenge expert evidence where such evidence is likely to determine the outcome of the proceedings. In all these cases ODR should promote international standards applied to analysed data, such as those published by international standards communities, like ISO

(International Organization for Standardization). The standardisation of communication patterns can produce considerable efficiency gains. See the guidelines on electronic evidence for further reference (in particular, guidelines no. 17 – 24 of the section on relevance of the electronic evidence).

Guideline 12

44. Specific challenges may arise when dealing with evidence in the courts using ODR mechanisms. These challenges point towards the need for consistency in the handling of the evidence. It is important to avoid discordant jurisprudence and to promote legal certainty. In this respect, parties may be allowed by their national legal system to rely on the previous decisions made by a court in similar or identical cases. This may help parties to have structured their evidence based on such previous decisions or on templates provided by the courts on the webpages. Specific recommendations may be issued by member States, for example on the format of the data to be submitted as evidence. Such solutions, however, should not undermine the independence of judges.

Effective proceedings

Guideline 13

45. As a large number of the judgments of the European Court of Human Rights relates to the violation of Article 6 of the European Convention on Human Rights in the context of referrals the excessive length of court proceedings, it is crucial for member States to increase their efforts in order to eliminate this problem. Effective proceedings require avoidance of undue delays. In this regard ODR provides advantage. Additionally, due to use of AI components the work of a court may be further significantly improved. The use of AI components may speed up the procedure and may allow for a more complete analysis of the case. Effective proceedings may be achieved only under condition that the process is streamlined as much as possible. In particular, physical presence of the parties should be required by the court only when it is necessary. ODR may assist in avoiding the necessity of physical presence not only of the parties themselves but also of other attendees, whose presence would otherwise be required, which often causes problems and slows down the proceedings. Many member States use videoconferencing in their courts with persons situated at a remote location to ensure, for example, an appearance of witnesses and experts. Proper design of the ODR also means that ODR allows payments of court fees on-line. See the guidelines on electronic evidence for further reference (in particular guidelines 1 – 5 of the section on oral evidence taken by remote link).

European Court of Human Rights' case-law

In requiring cases to be heard within a "reasonable time", the Court underlines the importance of administering justice without delays which might jeopardise its effectiveness and credibility (*H. v. France*, 24 October 1989, § 58, Series A no. 162-A; *Katte Klitsche de la Grange v. Italy*, 27 October 1994, § 61, Series A no. 293-B).

A state may be found liable not only for delay in the handling of a particular case, but also for failure to increase resources in response to a backlog of cases or for structural deficiencies in its judicial systems that cause delays. Tackling the problem of unreasonable delay in court

Guideline 14

46. Special attention needs to be paid to ensuring that proceedings are not unnecessarily protracted by technical difficulties. Alternatives have to always be available whenever the ICT system is under maintenance or is facing technical problems, in order to avoid any adverse impact on court activity. Such technical difficulties must not be detrimental to the parties and there should be a possibility to adjust time periods providing for a sanction, as necessary.

proceedings may thus require the state to take a range of legislative, organisational, budgetary and other measures (*Rutkowski and Others v. Poland*, nos. 72287/10 and 2 others, § 128, 7 July 2015).

Guideline 15

47. To ensure efficient, timely and adequate resolution of disputes and their de-escalation member States may integrate a pyramid model of dispute resolution where adjudication by a judge comes as a last tier. Amicable settlement of disputes with the involvement of ADR may further provide cost-efficient and more satisfactory result to parties than adjudication. However, attempts to settle a dispute with the involvement of ADR before instituting adjudicative proceedings before a judge shall be reasonable and should not compromise or deny access to court as a fundamental right protected by the Article 6 of the European Convention on Human Rights. Use of above-mentioned methods and techniques should not create substantial delay or increase substantively the costs for the parties.

Delivery of the decision

Guideline 16

48. The outcomes of the proceedings involving ODR being known to the parties is important for three reasons: (1) to ensure equality of information between the parties, (2) to ensure that the outcomes can be scrutinised and appealed if necessary and (3) to guide the development of the law. In case of ODR the most important factors are the public scrutiny and the requirement that the proceedings are conducted in a reasonable time, with due process.

Guideline 17

49. This guideline stems from the right to public delivery of judgment. Article 6 (1) of the European Convention on Human Rights explicitly states that judgment shall be pronounced publicly. However, this does not require reading out of the judgment in open court. Other means of rendering a judgment public are allowed, such as making judgments available on request (*Moser v. Austria*, no. 12643/02, § 101, 21 September 2006). In each case the form of publicity must be assessed in the light of the special features of the proceedings in question (*Pretto and Others v. Italy*, 8 December 1983, § 26, Series A no. 71; *Axen v. Germany*, 8 December 1983, § 31, Series A no. 72). For example, the full text of the judgment can be made available on the court website. According to the jurisprudence of the European Court of Human Rights the requirement for public pronouncement has been complied with where, by being deposited in the court registry, the full text of the judgment has been made available to everyone (*Pretto and Others v. Italy*, cited above, §§ 27-28).

Right to a reasoned decision

Guideline 18

50. Every judicial decision reached using ODR or with the assistance of ODR needs to be clear in order to allow everyone involved to understand why the court is supporting a certain position (*Seryavin and Others v. Ukraine*, no. 4909/04, §§ 55-62, 10 February 2011). ODR does not suspend the right to obtain an explanation for the decision taken. Sufficiently detailed reasons should be given. The extent of the duty to give reasons depends on the nature of the decision and the circumstances of the case. The main arguments of the parties should be examined and require a specific and explicit response. Sufficiently reasoned decisions are required, firstly, in order to reassure the parties that their respective arguments have been taken into account in arriving at the decision and, secondly, to assist a party in deciding whether there are sufficient grounds to appeal against the decision. It is only by giving a reasoned decision that there can be public scrutiny of the administration of justice. This means that, at the very least, the outcomes must be known to the parties.

Enforcement of the decision

Guideline 19

51. Execution of a final and binding decision which results from an ODR mechanism must be regarded as an integral part of the "right to a court" for the purposes of Article 6 of the European Convention on Human Rights. Every litigant to the ODR has a right to enforcement of a judgment, and the delay in the execution of a judgment must never be such that it impairs the litigant's right to a fair trial. The right to the execution of judicial decisions is of even greater importance in the context of administrative proceedings (*Sharxhi and Others v. Albania*, no. 10613/16, § 92, 11 January 2018). ODR can contribute to expediting enforcement proceedings in the same way as it can expedite the adjudicative stage of proceedings. For

example, national law may provide for the electronic enforcement clause sent directly through the IT system to the bailiff. Electronic communication with the bailiff makes it quicker and easier to monitor the execution of judicial decisions.

European Court of Human Rights' case-law

It would be inconceivable that Article 6 (1) should describe in detail procedural guarantees afforded to litigants – proceedings that are fair, public and expeditious – without protecting the implementation of judicial decisions (...) Execution of a judgment given by any court must therefore be regarded as an integral part of the "trial" for the purposes of Article 6 of the European Convention on Human Rights (*Burdov v. Russia*, no. 59498/00, § 34, CEDH 2002-III). An unreasonably long delay in enforcement of a binding judgment may therefore breach the Convention (*Burdov (n° 2)*, no. 33509/04, § 66, CEDH 2009).

National example: Lithuania

The majority of court order proceedings regarding monetary claims are handled using online filling and digital case management. Court orders are generally issued as digital official documents with secure electronic signatures that can be submitted electronically to the bailiff for enforcement.

Right to judicial review in cases involving purely automated decisions

Guideline 20

52. There can be no single, or simple, answer to the question concerning how the right to review a decision involving an ODR element should be exercised because it depends on the character and the scope of the ODR element concerned. Where the ODR only plays a subordinate role helping a judge in the proceedings, there is no reason to deviate from the standard rules on appeal applicable to proceedings not involving an ODR element. However, the question becomes crucial when ODR instruments take the shape of tools for purely automated decisions. The scenarios in which ODR mechanisms leading to purely automated decisions could be used extend from minor cases which can be easily automated because they are legally simple and the ODR mechanism is primarily used for calculation purposes, to complex cases involving advanced AI mechanisms.

53. However, it is in this context that Article 13 of the European Convention on Human Rights comes into play. Article 13 provides that everyone whose rights and

freedoms as set forth in the European Convention on Human Rights are violated shall have an effective remedy before a national authority. Parties should be allowed to contest purely automated decisions and to request that such review is to be made by a judge. The European Court of Human Rights does not specify at what level this remedy is to take place.

Basically, two models are conceivable: it is for the member State to decide if the review should be made at the same judicial level or at a higher appeal level. The use of ODR can open up new avenues of redress for infringements in the national judicial systems. In view of the unique character of the ODR the member State may decide, irrespective of existing review mechanisms, to establish an additional review process on the same level as the one, on which the automated decision was made. Alternatively, the member State can leave the review before a judge to its existing appeal level. In any case, this guideline does not require all automated decisions to be automatically subject to review or to change the existing review model.

European Court of Human Rights' case-law

Article 13, giving direct expression to the States' obligation to protect human rights first and foremost within their own legal system, establishes an additional guarantee for an individual in order to ensure that he or she effectively enjoys those rights (*Kudła v. Poland* [GC], no. 30210/96, § 152, CEDH 2000-XI).

Consultative Council of European Judges – Opinion No. (2011) 14

The introduction of IT in courts in Europe should not compromise the human and symbolic faces of justice. (...) Justice is and should remain humane as it deals primarily with people and their disputes.

Transparency in the use of ODR and requirements for hearings*Transparency in the design and operation of ODR mechanisms*

Guideline 21

54. Transparency in ODR is crucial. Both the design and operation of ODR mechanisms need to be explained to the public, in an easy- understandable language, in order to promote access to justice. The public should understand the implications of the use of ODR, believe that the ODR works well and that its outcomes are fair. This guideline goes beyond a simple requirement to disclose basic information on the design and use of ODR on the Internet. Different methods can be used to engage the public. Genuine communication strategies and policies includes press releases, video broadcasts, and webinars or social media publications. Member States can explain to the public that ODR makes justice more accessible, e.g. by not requiring the physical presence at the court, saving the costs of the travel to the court and allowing the parties to file documents by electronic means or ensuring confidence and reducing stress for individuals representing themselves in the proceedings.

Public and oral hearings

Guideline 22

55. In case of a traditional court (physical court buildings) its activity is self-explanatory to the public and can be inspected by members of the public by attending public hearings. It might be different when proceedings or separate hearings are performed remotely and electronically with the help of ODR mechanisms. One should remember what the aim of public hearings is: they allow for public scrutiny of judicial decisions and proceedings. Making proceedings transparent in this way is a form of accountability that enhances fairness. This function of public scrutiny must also be ensured in remotely conducted electronic proceedings using ODR tools. Here, these aims can be achieved by traditional and new means. Technically, digital courts can be designed as open courts, if not more so than physical court buildings. The particular technical solution depends on the design of the procedure in question. For example, where virtual hearings in the courts replace a court hearing, ODR may allow public access to virtual hearings and information in a controlled manner without the observers having to physically go to a courtroom. Organising traditional public hearing is not required in ODR but it might be used to ensure publicity of hearings while using ODR tools for remote (virtual) attendance of hearings by parties, witnesses, experts or some of them; judges and/or observers at the same time might be physically present in courtrooms or any other physical rooms where court hearings might be broadcasted. In any case, however, the requirement of public hearing does not require member States to open up their virtual hearings to an unlimited number of simultaneous streams to the public, just as much as seats in a physical courtroom are also limited. Any such option must consider the due safeguards in respect of protection of personal and other sensitive data, sufficient cybersecurity and other principled discussed in these guidelines.

Guideline 23

56. The purpose of ODR is not to close the courts and hearing rooms. The aim is to improve effectiveness and efficiency. The right to an oral hearing does not necessarily require physical presence, and videoconferencing may be an appropriate way to guarantee litigants their right for example where parties voluntarily renounce their right to a physical presence (*Vladimir Vasilyev v. Russia*, no. 28370/05, § 81-90, 10 January 2012). Videoconferencing where the communicators can hear and see each other in real time (and where provision is made that, for example witnesses are not coached from behind the screen and that witnesses' identity is properly authenticated) may, depending on the case, function as well as an "oral" hearing (provided the technology works on both ends of the transmission and this can be archived). An oral hearing is not always necessary to secure the parties participation in the proceedings. Written proceedings using ODR mechanisms can be permissible provided that the litigants have the right to have an oral hearing in the form of a review on the same level or re-hearing at an appeal stage of the proceedings. For instance, in administrative proceedings, an oral hearing before the authority is obligatory only in certain cases, and more emphasis is placed on the broadly understood right to active participation in

proceedings at any stage of the proceedings. Such participation does not require oral hearings, but the possibility of expressing the party's opinion on the materials in the case-file, including evidence collected and motions lodged by the other party (*Vilho Eskelinen and Others v. Finland* [GC], no. 63235, § 74, ECHR 2007-II). Using ODR can enhance the efficiency of written proceedings.

Other issues of transparency, including public scrutiny

Guideline 24

57. Safeguards for independence and impartiality of the judiciary must be effectively incorporated into proceedings involving ODR (*Agrokompleks v. Ukraine*, no. 23465/03, § 136, 6 October 2011). ODR must be transparent in terms of the identities and affiliations of the ODR providers and those of the interveners and managers of the ODR mechanisms. Member States should adopt policies dealing with identifying and handling conflicts of interest in the ODR.

Guideline 25

58. The guarantees enshrined in Article 6 (1) of the European Convention on Human Rights include the obligation that all documents generated by ODR, including the final judgment and other decisions or notifications, are written in clear and plain language. The language used must be such as to enable the parties to make effective use of any existing right of appeal.

Guideline 26

59. Procedural rules applicable to ODR should make clear the process used to resolve a dispute. These rules should meet the requirements of the society, institution, and legal frameworks they serve. In particular ODR should incorporate procedures for addressing factors which may harm the fair use of ODR. For example, an ODR may need to display or conceal different parts of information depending on the stage of process and the type of user. In this respect ODR can learn from a range of measures to mitigate risks and improve security, commonly used in other sectors including banking, online payment systems and healthcare sectors. These procedures need to be factored into the ODR's architecture.

Guideline 27

60. Relevant information can be made available on the court website in a user-friendly and accessible manner. For example, a court website may use text-to-audio transcription services. Good ODR information management ensures that information is authentic and reliable, can be retrieved quickly and easily, is retained for an appropriate length of time, is disposed of securely and appropriately, and is suitably protected. Transparency of procedural rules applicable to ODR contribute to increased trust, accountability, openness and efficiency.

Special issues related to the ICT nature of ODR techniques

Cybersecurity

Guideline 28

61. The justice system is vulnerable because of the increasingly sophisticated and numerous cyber-attacks to which courts are exposed. With the use of ODR comes the fear of an increase in the number of security breaches that would jeopardise the integrity of the judicial system and the data it handles. Cyber threats are a very real danger for justice systems. Risk exists that court documents and evidence can be subject to manipulation and attack. A breach in security could result in forgery, or the disclosure of confidential information. Against this background, courts may consider mechanisms for enhancing data security. There are ways of preventing such breaches in ICT (e.g. by reducing the risk of an attack occurring) and/or mitigating their effects (e.g. by planning in advance the right course of action in the event of an attack). It is crucial that an appropriate level of cybersecurity in the ODR systems and their integrity are ensured by member States. ODR mechanisms require protection to prevent external parties from hacking the system and obtaining non-public information. Regarding the authority to access information,

there should be internal limitations to ensure that parties to disputes cannot access information that they are not allowed to obtain. This requires secure authentication and access control.

62. The Appendix to this explanatory memorandum contains a cybersecurity checklist for member States.

Guideline 29

63. It is important that security is built into the design of the ODR. Security is to be ensured throughout the lifetime of the ODR mechanism by design and development processes that constantly evolve to reduce the risk of harm from malicious exploitation. There are two basic principles that need to be followed: the "security-by-design" and "security-by-default". The first means that all those involved in the design and development of ICT products, services and processes facilitating ODR are encouraged to implement measures at the earliest stages of design and development to protect the security of those products, services and processes to the highest possible degree, in such a way that the occurrence of cyber-attacks is presumed and their impact is anticipated and minimised. The principle of "security-by-design" is to be followed at the earliest stages of design and development to protect the security of ODR. The principle of "security-by-default" means that ICT products, services and processes facilitating ODR are configured in a way that ensures a higher level of security which should enable the first user to receive a default configuration with the most secure settings possible, thereby reducing the burden on users of having to configure an ICT product, service or process appropriately.

64. Certification plays a critical role in increasing trust and security in ICT products, services and processes facilitating ODR. This includes a comprehensive set of rules, technical requirements, standards and procedures. To express the cybersecurity risk, a certificate may refer to three assurance levels (basic, substantial, high) that are commensurate with the level of the risk associated with the intended use of the product, service or process, in terms of the probability and impact of an incident. The obtaining of certain certification levels may necessitate the existence of a national legal framework allowing and regulating testing and ethical hacking of (state-run) ICT systems.

Human rights protection, including personal data protection

Guideline 30

65. Member States' governments, legislators, courts as well as ODR developers, manufacturers and service providers should continuously assess the possible adverse consequences of ODR techniques and mechanisms on human rights and fundamental freedoms, and, considering these consequences, adopt a precautionary approach based on appropriate risk prevention and mitigation measures. In all phases of the processing, including data collection, they should adopt a "human rights by-design" approach and avoid potential biases, including those that may be unintentional or hidden, and risks of discrimination or other adverse impacts on the human rights and fundamental freedoms of individuals.

Guideline 31

66. It is necessary to ensure compliance of all processing of personal data using ODR mechanisms with data protection laws. The key underlying elements of this approach are the lawfulness, fairness, purpose specification, and proportionality of data processing. Responsibility for, and demonstration of, compliance (accountability), transparency, data security and risk management are also essential requirements.

Guideline 32

67. Personal data protection has to be a priority and needs to be properly resourced. Inadequate protection may hamper access to the courts. This risk should be counter-balanced by personal data protection training for court staff, clear data protection policies and guidelines, data protection audits and effective implementation of their results. Contemporary data protection regimes (such as the updated Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)) play an important role in safeguarding the rights and interests of data subjects. Special consideration should be given by member States to the Guidelines on Artificial Intelligence and Data

Protection adopted in 2019 by the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) of the Council of Europe.

68. "Technical and organisational measures", in the sense of these guidelines, are the functions, processes, controls, systems, procedures and measures taken to protect and secure the personal data that is processed within ODR system. These measures are a requirement for security of processing, preventing breaches, ensuring suitable processors, records of processing activities, design and a strong foundation for ensuring that rights and freedoms of the ODR users are protected. Specific measures include among others: i) protection against unauthorised access to confidential data, such as personal data, undisclosed know-how and business information, or other types of potentially sensitive information collected during ODR proceedings; ii) ensuring integrity of the data in order to exclude possibility of the unwanted alteration or deletion of data concerning electronic procedural documents, including the decision itself or pieces of evidence; iii) identification of fraud by parties, since the online context could make it harder for a judge to ascertain the identity of a party.

Guideline 33

69. ODR implementation can pose a threat to the privacy of individuals and should, therefore, be complemented by ethical and human rights considerations. There should be an appropriate balance between the utility of open data and the privacy of the data subjects. ODR mechanisms should be designed and developed responsibly, by applying the principles of "privacy-by-default" and "privacy-by-design". "Privacy-by-default" means that the court must ensure that personal data is processed with the highest privacy protection and "privacy-by-design" means that ODR need to implement technical and organisational measures, at the earliest stages of its design, in such a way that safeguards privacy and data protection principles right from the start.

Guideline 34

70. There is a risk that, in order to reduce the cost of ODR implementation, member States decide to outsource ODR platforms to external providers in exchange for access to personal data of users. It is also possible that ODR is exploited by the companies that base their business model on tracking the data. Privacy concerns require that commercial tracking, profiling or targeting is not built into the design of ODR systems, because such activities have potentially serious impact on the personal freedom and autonomy of individuals and may lead to prejudice and discrimination. Where all or any part of ODR mechanisms are outsourced, providers should be bound by a comprehensive processing contract which will guarantee compliance with data protection law and exercise of individuals' data protection rights.

Other issues (not stemming from the jurisprudence of the European Court of Human Rights)

Testing, monitoring, upgrading, research and development

Guideline 35

71. To ensure technological advancements, member States are encouraged to stimulate progress in the ODR field by developing and maintaining such mechanisms themselves or stimulating non-governmental and/or private projects and programs. The development of ODR mechanisms should be funded, whenever this is appropriate and possible, by public bodies with the aim of enhancing public trust and confidence in ODR. The purpose of these funds may be the creation of an environment conducive to ODR development in accordance with Articles 6 and 13 of the European Convention on Human Rights. Changes in the field of cyber justice should be court-driven, not technology-driven. Relevant research can fill in gaps in legal and technical knowledge and improve functioning of ODR.

Guideline 36

72. The purpose of testing ODR is to evaluate its compliance with the specified legal, procedural and technical requirements. ODR testing, for example, might verify whether every type of user input produces the intended output across the ODR application. Testing should be based on quality factors like reliability, usability, integrity, security, capability, efficiency, portability, maintainability and compatibility. Sufficient piloting and adjustments before the deployment ensure efficiency and adequate added value. Close, on-going involvement of future users helps to minimise any discrepancies between the needs stated on paper and how the IT specialists address them in practice, and enables the proposed technical solutions to be reoriented, where feasible and without affecting the project schedule or cost. Trials at pilot sites provide an opportunity to learn from a series of initial users before approving the next stage of the project or rolling it out on a bigger scale.

Guideline 37

73. The proper design of an ODR mechanism needs a constructive dialog to be established between those developing technology and those responsible for adjudication. It is for member States to decide which stakeholders should be involved and to what extent, as it depends on the type of the particular ODR concerned. Some require more input from the stakeholders, such as involvement of AI components and some less. The judiciary should be actively involved in the testing and piloting phases. In this context it is also important to ensure that the design of ODR do not deprive judges of their decision-making capacity. However, judges are not the only professionals that could be involved in the design. The dialogue may include other stakeholders such as lawyers, court staff and court users. Technology developers should strive to better understand the justice system and collaborate with judges and court staff to ensure that ICT architecture meets the needs of both the courts and the public. The ODR's architecture also needs to be flexible, and ready to adjust to judicial case-law or practices. For further references see Guidelines on how to drive change towards Cyber justice [Stock-taking of tools deployed and summary of good practices] of 7 December 2016, European Commission for the Efficiency of Justice.

Guideline 38

74. ODR must remain at the current level of service delivery and technological innovation. Each ODR mechanism goes through a development life cycle from initial planning through to disposition. The ODR mechanism has a cyclical nature which means that it constantly improves through change and upgrading. Replacing the outdated hardware or software, security upgrades, and continuous improvement on a regular basis is needed. Each member State should define its own best practices for various stages of ODR development.

Awareness raising, training and education

Guideline 39

75. Awareness raising, training and education of individuals and legal entities is key to enable successful exploitation of ODR techniques and mechanisms and to ensure its development and use. Measures need to be in place to improve a range of basic to advanced digital skills of different socio-economic groups. These include digital skills for the elderly, and other target groups, such as persons with disabilities. As the main providers of court services and ODR mechanisms, public authorities also require adequate knowledge and skills. This includes competences to develop ODR mechanisms in a responsive design manner for communities and businesses in compatibility with the requirements of the European Convention on Human Rights in order to build and enhance public trust and confidence in ODR.

Committee of Ministers Recommendation Rec(2004)4 to member States on the European Convention on Human Rights in university education and professional training

The Committee of Ministers recommends, inter alia, that member States ascertain "the adequate university education and professional training concerning European Convention on Human Rights and the case-law of the Court exist at national level and that such education and training are included, in particular (...) as a component of the preparation programmes of national or local examinations for access to the various legal professions and of the initial and continuous training provided for judges, prosecutors and lawyers".

In the framework of its follow-up to Recommendation Rec(2004)4, the Drafting Group III of the Committee of experts on the system of the European Convention on Human Rights (DH-SYSC), stated inter alia that member States should notably enhance the effectiveness of such university education and professional training by providing each category of public with necessary tools to comply with the obligations stemming from the European Convention on Human Rights. To this end, member States should provide quality targeted and accessible professional training. Also, professional training should be provided, as far as possible, by persons having good knowledge of the system of the European Convention on Human Rights and practical experience from the relevant professional field (see document DH-SYSC-III(2019)01 Rev, §§ 2 and 5).

Guideline 40

76. Member States need to ensure that ODR mechanisms are user-focused, accessible, fair, transparent, accountable and financially viable. Judges, legal practitioners and all those involved in court proceedings should be aware that the use of ODR has a potential to lead to greater automation, greater speed of information processing, better efficiency and lower costs of dispute resolution. This means that more disputes can be resolved, leading ultimately to a greater access to dispute resolution and to cost savings. ODR also has the ability to revolutionise access to justice, for example to persons who would find it hard to access courts. The development of online learning methods could be used to disseminate such details of ODR experience among all professionals concerned.

Guideline 41

77. Access to interdisciplinary training on ODR operation is necessary for judges and legal practitioners as well as court staff. Dispute resolution professionals should have sufficient skills and training to carry out their duties. The digitally competent professional should be aware of advancements in technology and, in particular, keep abreast of developments within IT security. Experts generally underline the need for proper means of protection and control, and emphasise the importance of providing all court staff with IT security training for online communications. Member States should take measures to ensure legal and IT experts are available to judges, legal practitioners and court staff for consultation when specialised knowledge on the interpretation and application of laws and regulations is required in the process of providing ODR services.

Training on ODR may cover specific challenges raised by ODR, such as cybersecurity. Awareness of the wider digital context and use of emerging technologies, such as cloud computing, trust services or blockchain, is important.

Guideline 42

78. Judges are encouraged to be able to use ODR mechanisms and follow good practices in the handling of ODR. Such good practices address, e.g. the risk that certain individuals (with physical or mental disabilities, socially disadvantaged or the elderly) will find it difficult to obtain access to justice. In order to prevent this, judges are encouraged to consult extensively with lawyers who tend to serve traditionally disadvantaged or marginalised groups. Another risk is that the removal of discretion and human judgment could lead to prejudice and stereotyping. This risk can be also prevented by judges in the review process (see paragraphs 52-53 above). Judges are encouraged to be aware of and understand the data risks, security, and privacy issues.

Guideline 43

79. Law schools are encouraged to change, if necessary, the way they provide education and provide a digital lawyering skills framework to teach students how to use technology to assist in the delivery of legal services. Good practices include new models of learning, such as increased level of online learning developed during pandemic crisis. Legal education and the legal profession may follow such good practices in order to keep pace with technological advancements, in particular introduction of ODR mechanisms in the justice systems. It is important that students stay mindful of the legislation that governs human rights. Students need also be aware that courts are now utilising artificial intelligence to enhance their practices. In this respect a good practice is that students are given an opportunity to explore not only where the practice of law is now but also where it is heading. A broad range of competencies are required for an individual to be considered digitally competent. Teachers can use real-world examples.

APPENDIX

CYBERSECURITY CHECKLIST FOR MEMBER STATES

Member States should implement the following in designing ODR:

1. **Protection of stored, transmitted or otherwise processed data:**
 - a. against accidental or unauthorised storage, processing, access or disclosure during the entire life cycle of the ICT product, service or process facilitating ODR.
 - b. against accidental or unauthorised destruction, loss or alteration or lack of availability during the entire life cycle of the ICT product, service or process facilitating ODR.
2. **User access management through secure identification and authentication:** Authorised persons, programs or machines should only be able to access the data, services or functions to which their access rights refer.
3. **Identification and documentation of known dependencies and vulnerabilities:**
 - ⇒ Modern ICT products and systems often integrate and rely on one or more third-party technologies and components such as software modules, libraries or application programming interfaces. This reliance, which is referred to as a "dependency", could "pose additional cybersecurity risks as vulnerabilities found in third-party components could also affect the security of the ICT products, services and processes facilitating ODR. In many cases, identifying and documenting such dependencies enables end users of ICT products, services and processes to improve their cybersecurity risk management activities by improving, for example, users' cybersecurity vulnerability management and remediation procedures.
 - ⇒ Additionally, such dependencies and vulnerabilities could to a certain degree be avoided by providing, to the extent possible, the necessary means for in-house design and development.
4. **Logging of data accession, use and processing:** to record which data, services or functions have been accessed, used or otherwise processed, at what times and by whom.
5. **Allowing consultation of the log files:** to make it possible to check which data, services or functions have been accessed, used or otherwise processed, at what times and by whom.
6. **Vulnerability testing:** verifying that ICT products, services and processes facilitating ODR do not contain known vulnerabilities.
 - ⇒ Vulnerability testing may necessitate the existence of a national legal framework allowing and regulating testing and ethical hacking of (government) ICT systems.
7. **Providing back-up facilities and technical support:** to restore the availability and access to data, services and functions in a timely manner in the event of a physical or technical incident.
8. **Security-by-design and by-default:** that ICT products, services and processes facilitating ODR are secure by-design and by-default.
9. **Up-to-date hard- and software:** to ensure that ICT products, services and processes facilitating ODR are provided both with up-to-date software and hardware that do not contain publicly known vulnerabilities, and with mechanisms for secure updates.

Cybersecurity certification of ICT products, services and processes facilitating ODR could be sought in order to minimise cybersecurity risks and to maximise trust and confidence. E.g. for EU-countries: certification could be sought in the framework of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (European Union Cybersecurity Act).

BIBLIOGRAPHY

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.

Online Dispute Resolution and Compliance with the Right to a Fair Trial and the Right to an Effective Remedy (Article 6 and 13 of the European Convention on Human Rights). Technical Study on Online Dispute Resolution Mechanisms. Prepared by Prof. Julia Hörnle, CCLS, Queen Mary University of London, Matthew Hewitson (South Africa) and Illia Chernohorenko (Ukraine), Strasbourg, 1 August 2018, CDCJ(2018)5.

Guide on Article 6 of the European Convention on Human Rights, Right to a fair trial (civil limb), updated on 31 August 2019, Council of Europe/European Court of Human Rights, 2019.

A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework. Prepared by the Expert Committee on human rights dimensions of automated data processing and different forms of artificial intelligence (MSI-AUT). Rapporteur: Karen Yeung, DGI(2019)05.

Guidelines on Artificial Intelligence and Data Protection, T-PD(2019)01.

European Ethical Charter on the use of artificial intelligence in judicial systems and their environment, Council of Europe, Commission for the Efficiency of Justice (CEPEJ), 3-4 December 2018.

"European judicial systems, efficiency and quality of justice: Use of information technology in courts in Europe", CEPEJ Studies No. XX, 2016 edition (2014 data).

Consultative Council of European Judges (CCJE), Opinion No. (2011)14, "Justice and information technologies (IT)".

Drafting Group of the Committee of experts on the system of the European Convention on Human Rights (DH-SYSC), Drafting Group III on the follow-up to Recommendation Rec(2004)4, Good national practices illustrating the principles set in Appendix I to the revised Recommendation Rec(2004)4 (document DH-SYSC-III(2019)01 Rev), 2019.

Magna Carta of Judges, Council of Europe, Consultative Council of European Judges (CCJE), 2010.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108); see <http://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1> [Accessed 20 November 2020].

Parliamentary Assembly of the Council of Europe, Resolution 2054 (2015), "Access to justice and the Internet: potential and challenges", Report: Doc. 13918 of 10 November 2015.

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881&from=EN>) [Accessed 20 November 2020].

Recommendation of the OECD Council on Artificial Intelligence, OECD/LEGAL/0449, Adopted on: 22 May 2019, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449> [Accessed 20 November 2020].

The European Commission's high-level expert group on artificial intelligence, A Definition of AI: Main Capabilities and Scientific Disciplines. Definition developed for the purpose of the deliverables of the High-Level Expert Group on AI Brussels, 18 December 2018; <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai> [Accessed 20 November 2020].

Byrom N., Digital Justice: HMCTS data strategy and delivering access to justice. Report and recommendations, The Legal Education Foundation, October 2019.

Hörmle J., Cross-border Internet Dispute Resolution, Cambridge University Press 2009.

Hörmle J., Encouraging Online Alternative Dispute Resolution (ADR) in the EU and Beyond, European Law Review 2013, Volume 38 (2), pp. 187-208.

UNCITRAL Technical Notes on Online Dispute Resolution, New York, 2017.

Online Dispute Resolution Standards of Practice as developed by the ICANN available at <https://www.icann.org/en/system/files/files/odr-standards-of-practice-en.pdf> [Accessed 20 November 2020].

UNCITRAL Working Group III (Online dispute resolution) Thirty-third session, New York, 2016, Online dispute resolution for cross-border electronic commerce transactions, A/CN.9/WG.III/WP.140, <https://undocs.org/en/A/CN.9/WG.III/WP.140> [Accessed 20 November 2020].

Rainey B. et al, Jacobs White & Ovey, The European Convention on Human Rights, Oxford University Press, 2014.

Carneiro D. et al., ODR: an Artificial Intelligence Perspective, Artificial Intelligence Review 2014, Volume 41, pp. 211-240.

Altreas N. et al, Predicting judicial decisions of the European Court of Human Rights: a Natural Language Processing perspective, Peer J Computer Science Open Access (Published 24 October 2016) <https://peerj.com/articles/cs-93.pdf> [Accessed 20 November 2020].

Loutocký P., Online dispute resolution and the latest development of UNCITRAL model law, in: Cofola International 2015: current challenges to resolution of international (cross-border) disputes: conference proceedings (ed. K. Drličková), Brno 2015, pp. 243-256.

Scherer M., Artificial Intelligence and Legal Decision-Making: The Wide Open?, Journal of International Arbitration 2019, vol. 36, no. 5, pp. 539-574.

Hanriot M., Online dispute resolution (ODR) as a solution to cross border consumer disputes: the enforcement of outcomes, McGill journal of dispute resolution 2015, Volume 2, pp. 1-22.





Uzelac A., van Rhee C. H. (eds.), Transformation of Civil Justice, Ius Gentium: Comparative Perspectives on Law and Justice, Springer International Publishing 2018.

Vitkauskas D. and Dikov G., Protecting the right to a fair trial under the European Convention on Human Rights: A handbook for legal practitioners, Council of Europe 2017, available from: <https://rm.coe.int/protecting-the-right-to-a-fair-trial-under-the-european-convention-on-/168075a4dd> [Accessed 20 November 2020].

Related documents





CM(2021)36-add2final

European Committee on Legal Co-operation (CDCJ) - c. Guidelines of the Committee of Ministers of the Council of Europe on the efficiency and the effectiveness of legal aid schemes in the areas of civil and administrative law

 DOCX  31/03/2021  English  CM-Public

CM(2021)36-add1

European Committee on Legal Co-operation (CDCJ) - b. Study on the feasibility of a new, binding or non-binding, European legal instrument on the profession of lawyer – possible added-value and effectiveness

 DOCX  03/03/2021  English  CM-Public

CM(2021)36

European Committee on Legal Co-operation (CDCJ) - a. Abridged report of the 95th

plenary meeting (4-5 and 23-24 November 2020, via videoconference)[DOCX](#) [03/03/2021](#) [English](#) [CM-Public](#)**CM/Del/Dec(2021)1400/10.2**

European Committee on Legal Co-operation (CDCJ) - a. Abridged report of the 95th plenary meeting (4-5 and 23-24 November 2020) - b. Study on the feasibility of a new, binding or non-binding, European legal instrument on the profession of lawyer - possible added-value and effectiveness - c. Guidelines of the Committee of Ministers on the efficiency and effectiveness of legal aid schemes in the areas of civil and administrative law and Explanatory Memorandum

[DOCX](#) [31/03/2021](#) [English](#) [CM-Public](#)**CM(2021)36-add3final**

[1400/10.2c] European Committee on Legal Co-operation (CDCJ) - Guidelines of the Committee of Ministers of the Council of Europe on the efficiency and the effectiveness of legal aid schemes in the areas of civil and administrative law - Explanatory Memorandum

[DOCX](#) [31/03/2021](#) [English](#) [CM-Public](#)**CM(2021)36-add4final**

Guidelines of the Committee of Ministers of the Council of Europe on online dispute resolution mechanisms in civil and administrative court proceedings (Adopted by the Committee of Ministers on 16 June 2021 at the 1407th meeting of the Ministers' Deputies)

[DOCX](#) [16/06/2021](#) [English](#) [CM-Public](#)

1407th meeting of the Ministers' Deputies (16 June 2021) - M... 22/03/2021
www.coe.int/.../june-2021?p_p_id=101_INSTANCE_FJJUjash2rEF&p_p_...

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