CM-Public

MINISTERS' DEPUTIES CM Documents **CM(2022)10-final** 9 February 2022

1424th meeting, 9 February 2022

2 Current Political Questions

2.4 European Committee on Democracy and Governance (CDDG)

b. Committee of Ministers' Guidelines on the use of information and communication technology (ICT) in electoral processes in Council of Europe member States

Committee of Ministers' Guidelines on the use of information and communication technology (ICT) in electoral processes in Council of Europe member States

Introduction

Free and fair elections and referendums are one of the cornerstones of democracy. The integrity of the electoral process is fundamental to maintaining public trust in the legitimacy of democratic institutions.

There is a current trend to increasingly rely on information and communication technologies (ICTs) in all spheres of life, including in election administration. These guidelines aim to contribute to ensuring the integrity of the electoral process and therefore enhancing citizens' trust in democracy. The guidelines identify requirements and safeguards to be introduced into the legislation of Council of Europe member States in order to address the use of ICTs in the different stages of the electoral process.

Scope of the guidelines

Countries may choose to use ICT solutions to handle electoral data and processes such as:

- registers and the registering of voters, observers, the media, etc.;
- the collection of e-signatures in support of questions (initiatives or petitions, for example), candidates or parties;
- the online publication of election-related information;
- the e-transmission of election data between local, regional and central electoral authorities;
- the online training of election staff and other stakeholders or the e-accreditation of observers;
- the determining, processing, transmitting and publishing of election results;
- the observation of different election-related activities, etc.

In addition, ICT solutions have been discussed in the context of the Covid-19 pandemic, as the regular conduct of the electoral process has been affected.

E-data and e-processes may improve the exercise of political rights by offering better accessibility, more opportunities for interaction, and increased transparency for example. There may also be advantages for election administration in terms of speed, efficiency, or accuracy. At the same time, the implementation and use of ICTs also increase complexity and heighten the exposure to threats and risks inherent in the ICT solutions or systems employed.

These guidelines cover the use of ICT solutions by, or on behalf of, the relevant electoral authorities, in all the stages of the electoral process except e-voting and e-counting, which are covered by CM/Rec(2017)5 on standards for e-voting and are thus beyond the scope of these guidelines. However, hybrid forms of counting, which make use of some ICTs but do not fall within the definition of e-voting according to CM/Rec(2017)5, are covered by the current guidelines. The use of ICTs by others in the context of the electoral process, namely campaigning activities such as political microtargeting by political parties or information provided by media outlets, is not addressed by these guidelines.

Core principles of democratic elections and referendums

The use of ICT, like the use of any other technology in electoral processes, should comply with the principles of democratic elections and referendums and other relevant principles and must be balanced against other core considerations such as security and accessibility for users.

Democratic elections and referendums should be held in accordance with certain principles that grant them their democratic status. The Code of good practice in electoral matters of the European Commission for Democracy through Law (Venice Commission),[1] adopted in 2002, is the reference document of the Council of Europe in the field. It defines the "European electoral heritage" from two aspects: the fundamental constitutional principles of electoral law and certain basic conditions necessary for their application.

In line with the 2002 Code of good practice in electoral matters, the meaning of the core electoral principles and conditions can be summarised as follows:

- "universal suffrage": all human beings have the right to vote and to stand for election subject to certain conditions, such as age, nationality or residence;
- "equal suffrage": each voter has the same number of votes; each vote has the same weight and the equality of opportunity must be ensured;
- "free suffrage": the voter has the right to form and to express his or her opinion in a free manner, without any coercion or undue influence;
- "secret suffrage": the voter has the right to vote secretly as an individual, and the State has the duty to protect that right;

- "direct suffrage": the ballots cast by the voters directly determine the person(s) elected;
- "frequency of elections": elections must be held at regular intervals;
- "respect for fundamental rights": democratic elections require respect for human rights, such as freedom of expression, freedom of movement, freedom of assembly and freedom of association;
- "regulatory levels and stability of electoral law": rules of electoral law must have at least the rank of a statute; rules on technical matters and detail may be included in regulations of the executive. The fundamental elements of electoral law should not be open to amendment less than one year before an election, or should be written into the constitution or at a level higher than ordinary law;
- "procedural guarantees": these include procedural safeguards aimed at ensuring the organisation of elections by an impartial body, the observation of elections by national and international observers and an effective system of appeal, among other things;

These guidelines are general and intended for any use of ICTs in the envisaged stages of the electoral process. In addition to the core electoral principles and respect for fundamental rights, democratic elections and referendums should comply with all other relevant legal principles. These include relevant international obligations, recommendations and standards, namely on elections and ICT, such as those mentioned in the preamble to Recommendation CM/Rec(2017)5 on standards for e-voting. Furthermore, relevant legal principles are to be found at the national and sub-national levels.

Furthermore, security (of the data and the system) should be considered as one of the guiding principles that informs the design, development, and deployment of ICT solutions at all stages of the electoral process, thus ensuring a human-centred security-by-design approach. For instance, ensuring integrity and authenticity, availability and reliability, secrecy and confidentiality, and usability and accessibility implies that the system and the information are secured against potential risks that would compromise these goals. Hence, any risk assessment should be adjusted to the phase of the election cycle it concerns. Conducting continuous risk management based on predefined criteria for risk acceptance and a predefined methodology is an important part of the effort to ensure security. ICT solutions used should be state-of-the-art and be based on peer-reviewed algorithms and concepts that are broadly endorsed by the respective scientific community. This can increase trust in the process.

Interdisciplinarity is strongly recommended when regulating the use of ICT solutions in the electoral process as it positively affects the quality of the regulation. Furthermore, the guidelines build upon the lessons learned from the use of e-voting and e-counting by member States, as well as upon good practice.

General guidelines applicable to all considered stages of the electoral process

In the following guidelines, "member State" refers to the authority in charge of regulating, conducting or supervising the electoral process in question. Usually, but not always, it refers to the electoral management body at the local, regional, or central level. It may also refer to other public institutions such as the parliament or the government, as the case may be.

1. Member States should ensure that ICT solutions respect the principles of democratic elections and referendums, and that sufficient consideration is given to other relevant principles.

General legal principles that apply to the different phases of the electoral process should be identified. It is often not possible – even with paper-based, or manual, solutions – to implement all principles to the same degree. This could be for two main reasons:

there might be a real or perceived conflict between principles (between secrecy and data protection on one side and transparency on the other, for example) for which a balanced level to which each of them should be ensured needs to be defined.

solutions, be they on paper and manual or based on ICT, usually rely on assumptions (such as assumptions about users' interactions with each other or with the ICT, or assumptions about the capability of potential attackers). Only if these assumptions hold true can the principles and derived requirements be ensured. If the assumptions are not realistic, it is very likely that the principles will be compromised and/or violated.

Thus, besides identifying the general legal principles that apply, it is important to define the minimum level to which they should be ensured. Furthermore, assumptions should be analysed as part of regular risk assessment (see Guideline 9) and should give sufficient consideration to security concerns.

Detailed legal and technical requirements that apply to ICT solutions should be derived from the identified legal principles. The corresponding minimum levels to which they should be ensured, need to be defined. The technical requirements should include functional and non-functional requirements (for example, maintenance and interoperability requirements in addition to those concerning security, usability, and accessibility) as well as assumptions. For technical requirements it should be indicated which assumptions are acceptable and which are not (usually because they are not realistic). The definition of minimum levels should include a list of assumptions. The technical requirements and assumptions should be written in a technology-neutral way.

The development and decision process for deducing technical requirements, including minimum levels and assumptions that might be acceptable, should be documented, include information about the people involved (most likely an interdisciplinary team) and be made publicly available, ensuring a transparent process.

Regulation should indicate what complaints and dispute-resolution mechanisms are available in relation to the use of ICT solutions and should address how to handle possible claims about irregularities.

2. Member States should ensure the usability and the accessibility of ICT solutions used in the electoral process by applying a human-centred approach.

Usability criteria for ICT solutions are defined in ISO standard 9241, for example.[2] The user interfaces intended for wider groups of people, especially voters, should be designed following stricter criteria than those intended for small groups of expert users, such as election officials. Accessibility requirements should take user needs into account and ensure that ICT solutions are accessible to all people (whether they have a

disability or not). Usability and accessibility thus complement each other. The legal and technical requirements for usability and accessibility and the minimum level to which requirements need to be met should be defined following Guideline 1. This second guideline deals with the development process.

A human-centred approach should be taken when developing ICT solutions for use in the electoral process. This means that from the beginning, (future) users of the ICT solution should be involved throughout the entire development and design process. They can be involved through semi-structured interviews and focus groups, via opportunities to provide feedback (on paper) on mock-ups and processes, and through user studies. A human-centred approach also includes conducting surveys, once the ICT solution is in use in the electoral process, to collect feedback from the field to further improve the usability and accessibility over time.

3. Where member States choose to provide an e-solution which is not universally accessible, an alternative, broadly accessible solution should also be provided.

Universal suffrage implies that all electoral stakeholders can accomplish all tasks and exercise all rights, as foreseen by the law. Having a parallel, equivalent procedure, accessible to most users, may be necessary in cases where the ICT solution is not universally accessible. It should also be noted that in some cases the use of ICT can be more accessible to some people than traditional paper-based solutions.

By maintaining an alternative procedure in addition to one using ICT, member States ensure that all stakeholders entitled to universal suffrage have access and thus avoid creating or deepening the digital divide. This implies that potential users are identified, accessibility is assessed, and an alternative and broadly accessible solution is developed and maintained. The public should be informed about the alternative solution.

Regulation should clarify the legal value of the results produced by co-existing alternative solutions as well as the applicable rules in case they are used by the same person. Furthermore, regulation should clarify how to deal with conflicts and other possible issues arising from the use of multiple channels for the same process.

4. Member States should ensure the integrity and authenticity of the information provided by ICT solutions used in the electoral process. Procedures should be put in place to detect and, if possible, correct any errors or unauthorised intervention.

ICT solutions should implement authentication mechanisms to avoid unauthorised changes according to the assumptions defined as part of Guideline 1. ICT solutions in the electoral process should operate without errors or unauthorised changes, thus contributing to the integrity of the election. The organisation of the election should provide for accurate checks and balances throughout all relevant election phases. Such integrity checks are essential parts of the overall security and cybersecurity efforts to protect the elections against attacks, from external attackers and/or unauthorised internal access, and of the efforts to address potential mishandling or errors in software or hardware. Protocols should be in place to detect and respond effectively to such incidents. The checks should be carried out with an appropriate degree of independence.

Ideally, any unauthorised changes or errors in the e-process or e-documents should be detected and corrected. If that is not possible, assumptions should be formulated accordingly, as part of Guideline 1. The possibility to detect and correct errors or manipulations is important in all phases of the electoral process, including when handling voter rolls as well as in respect to tallying and the transmission of results from polling stations to a regional or central authority, especially if transmission is done via the internet.

Preferably, it should be possible to make someone accountable if unauthorised changes or errors occur. It is essential to provide for an accountable and transparent procedure concerning how to interact with a running system, correct any data, or change or replace a malfunctioning system. Interacting with a running system for such purposes should be addressed in the risk analyses (see Guidelines 1 and 9).

Stakeholders should be able to verify that the tallying and the transmission of results were done correctly, including but not limited to using statistical tests of numerical election results such as risk-limiting audits and different types of observations, informed by country-specific expertise.

5. Member States should ensure the availability and reliability of the ICT solutions used in the electoral process.

ICT solutions should be available and reliable. An ICT solution should be functional, in line with the requirements and assumptions even in the event of a system failure or errors by users or others, or in case of attacks. Furthermore, the ICT solution should be reliable. It should retain its functionality, irrespective of shortcomings in the hardware or software in other parts of the electoral process. Alternatively, measures should be in place to provide information about and to activate pre-established fallback solutions and channels, including solutions that do not rely on active connections.

Incident response and business continuity plans should be put in place and regularly tested. Security measures to ensure availability and reliability include (this list is not exhaustive) management of access rights to the system, procedures for testing the system before the actual election process, procedures for carrying out updates during the operation phase, security rules for transmitting information outside controlled environments, data-protection requirements, having the system identify irregularities, and communication in case of problems. This may include procedures as required by ISO standards such as the ISO 27000 series.

6. Member States should ensure the secrecy and confidentiality of information stored within the ICT solution, as required by election and data-protection laws.

Secrecy and confidentiality requirements derived from the relevant legal principles should be ensured, taking into account the assumptions, which should also be defined, as discussed in Guideline 1. This includes considerations about long-term secrecy, that is, whether or not secrecy should be assured over time (for example, given that it is possible to store encrypted data today and decrypt it later, with existing or new solutions, such as quantum computers, which are expected to become broadly available).

Data-protection principles such as privacy by design or data minimisation are minimum requirements and should be considered whenever ICT is used in the electoral process. Furthermore, for each specific ICT solution used, member States should consider whether additional, suitable, and specific measures that go beyond data-protection measures are needed to safeguard the fundamental rights of the data subject, as

required, for instance, by Article 6, paragraph 1, of the Council of Europe Convention for the Protection of Individuals with regard to the Processing of Personal Data (ETS No. 108). If the member State identifies a need for such specific measures, they should become part of the electoral regulations.

Conflicts between transparency on the one hand and confidentiality and secrecy on the other should be carefully considered (see also Guideline 7).

7. Member States should ensure transparency of the election and of the ICT solutions used.

Providing transparency in all aspects of an election is key to conducting a successful and trustworthy election, and to promoting trust in the process, even more so when ICT solutions are used. Increasingly, non-IT experts experience difficulties understanding ICT solutions. Therefore, there is a need to increase the capacity of all stakeholders for understanding the ICT solutions.

All relevant stakeholders should be informed about the use of ICT solutions, including their introduction into the election process, their operation and the post-election assessment of the use of the solution. Details about its introduction should include:

1. elaborating on the overall strategy;
2. publishing technical requirements, assumptions and information on how the requirements should be met;
3. addressing perceived shortcomings from previous elections;
4. communicating about the development and decision process, including the collected inputs and the (interdisciplinary) team involved;
5. providing information on the feasibility of the overall implementation;
6. providing information about the procurement of the solution and its organisation;
7. providing information about the exhaustive evaluation before starting to use the ICT solution, as well as information on the results of the continuous risk assessment;
8. providing information on how conflicting or competing principles such as privacy and secrecy versus transparency are to be addressed;
9. publishing the source code.

Transparency also includes providing observers with access to documentation and to the processes, ideally in a language familiar to them.

Further, transparency measures should also include provisions for structured (machine-readable) data about the election process (such as the location of polling stations and their opening hours, lists of candidates and election results), including as open data.

Transparency requirements should aim at enabling public scrutiny. Appropriate processes should be in place for receiving, answering or discussing feedback from the public and for processing the conclusions. In this way, transparency can contribute to the overall security of and trust in the electoral process.

Last, transparency is a cross-cutting theme and as such touches on other guidelines as well. It requires, among other things, publishing assumptions (Guideline 1); providing information about the development and decision-making process for establishing the usability and accessibility criteria (Guideline 2); organising a transparent procedure on how to interact with a running system, correct any data, or change or replace a malfunctioning system (Guideline 4); documenting decisions on availability and reliability, including the respective requirements (Guideline 5); documenting decisions on security and confidentiality, including decisions on reconciling them with transparency requirements (Guideline 6); documenting requirements for system evaluation (Guideline 8); or documenting the risk-management process (Guideline 9).

8. Member States should organise an evaluation of the ICT solutions used in the election process by independent experts prior to implementation.

This guideline deals with the process of evaluation prior to implementing an ICT solution in the election process. The evaluation should extend to, but not be limited to, security, usability, and accessibility aspects. Its scope should cover the whole ICT solution and its usage environment.

Evaluation approaches should be defined, including the evaluation assurance level. Ideally, preference should be given to a standardised evaluation approach. As a precondition, the target of the evaluation should be clearly defined.

The evaluation requires several documents which, in the case of a standardised evaluation, need to be clearly defined. It should be determined – at a very early stage – whether the evaluation is to be conducted only by selected experts with access to the ICT solution, the source code and documentation and/or whether an assessment (or parts of it) can be conducted by anyone because the ICT solution, source code and documentation are publicly available.

It should also be stipulated how an independent evaluation is to be reached. Experts should be as independent as possible. This can be accomplished if two entities are involved: one is mandated to conduct the actual evaluation and the other, a State organisation, supervises the evaluating entity. Different experts might be needed for different requirement areas (such as security or usability/accessibility). Finally, it is important to consider the time needed by independent experts to conduct the evaluation.

The evaluation requirements and approach, as well as the evaluation results and information about the entities/persons involved (most likely an interdisciplinary team), should be made publicly available.

9. Member States should conduct continuous risk management of the ICT solutions used in the election process.

Processes that are important for the correct holding of an election and delivering accurate outcomes might face risks similar to e-voting, in particular if the underlying solution is web-based. These risks should be managed. In particular, when security risks are identified, proportionate responses should be developed.

Risks should be deduced from the requirements and assumptions (Guideline 1) and the result of the evaluation (Guideline 8). Thus, risk management is relevant during the development process and while using the ICT solution in the electoral process, as well as when preparing future elections. Evaluating the current risks and deciding whether the remaining risks are still acceptable is a continuous process. This is of

particular importance as new types of attacks emerge over time.

It is important to be aware of the remaining risks. Furthermore, it should be decided if and how to manage these risks. Risk-management approaches should include contingency plans.

In the light of risk management, it should be decided what information should be made publicly available and what should not, bearing in mind that security through obscurity is generally regarded to be counterproductive.

The risk-management approach should be reconsidered on a regular basis, at least after each election. Any unusual cases, problems or complaints should be taken into account.

The risk-management approach, as well as the information about the entities/persons involved (most likely an interdisciplinary team), should be made publicly available.

10. Member States should build and retain the necessary capacity to assess, introduce and manage the use of ICT solutions in the electoral process.

When introducing ICT into any part of the electoral cycle, it is essential that member States have the necessary administrative and technical capacity and related resources, including financial resources, to plan, implement and run the technology successfully and in a sustainable way.

Member States should consider, among other things, the degree of automation of the entire electoral process and potential synergies between the new solution and existing low-tech or high-tech solutions. Ideally, they should have a broader strategy on ICT-related investments in place.

Administrative and technical capacity essentially requires a skilled labour force, which should be continuously trained, equipped with the necessary tools and resources and, most importantly, given enough time to focus on their tasks.

The ultimate goal of having the necessary capacities is to avoid outsourcing essential election administration tasks to third, for-profit parties and thus to enable the relevant authorities to effectively oversee the election in accordance with legal requirements, without being dependent on private parties.

11. Member States should be ultimately responsible, also when private stakeholders are involved.

When organising elections, the member State has the ultimate responsibility for the proper implementation and conduct of the electoral process. This is also the case when third parties (including private parties) support the member State in conducting the electoral process, or when parts of the electoral process are outsourced and/or subcontracted to third parties. Third parties must respect and fulfil the same standards and expectations as member States. Corresponding provisions should be included in the contractual arrangements.

12. Member States should proactively address the possible use of ICT solutions in situations where "force majeure" affects the regular conduct of elections.

Recent experiences of adapting electoral procedures to the new health-related restrictions imposed by the Covid-19 pandemic have highlighted the issue of introducing ICT solutions to help deal with such exceptional circumstances. However, as illustrated by these guidelines, the use of ICT solutions cannot be considered a short-term remedy for extraordinary situations. Instead, it should be part of longer-term planning of the electoral process and of a broader approach to dealing with exceptional events.

Member States should proactively address future disruptions, including pandemics. If member States intend to use ICT solutions in such extraordinary circumstances, they are advised to prepare in advance for such an eventuality, in line with the previously mentioned guidelines.

Glossary of some terms used in the guidelines

- **Accessibility:** accessibility is about designing products and systems that are accessible for everyone, whether a person has a disability or not. At the same time, accessibility may specifically address discriminatory aspects related to equivalent user experiences, focusing on people with disabilities to ensure inclusion.[3]
- **Assumption**: Assumptions describe conditions that the operational environment in which the ICT solution is used needs to meet, if it is to provide all of its security functionality. "If the Target of evaluation (TOE) [the ICT solution] is placed in an operational environment that does not meet these assumptions, the TOE may not be able to provide all of its security functionality anymore. Assumptions can be on physical, personnel and connectivity of the operational environment."[4] The Guidelines recommend transparency about the assumptions and their evaluation (see Guidelines 1 and 7). Their "realistic/unrealistic" status should be periodically re-evaluated (see Guideline 9 on risks management policy).
- **Authenticity (of the information)**: the property that data originated from its purported source.[5]
- **Availability**: ensuring timely and reliable access to and use of information and systems.[6]
- **Elections**: political election or referendum.
- **Human-centred (design)**: (as used in ISO standards) is an approach to problem solving, commonly used in design and management frameworks, that develops solutions to problems by involving the human perspective in all steps of the problem-solving process. Human involvement typically takes place in observing the problem within context, brainstorming, conceptualising, developing and implementing the solution.[7]
- **ICT**: information and communication technology. In these guidelines, it equates to products and processes that store, retrieve, manipulate, transmit or receive information electronically in a digital form.
- **Integrity (of the information)**: the property that data have not been altered in an unauthorised manner. Data integrity covers data in storage, during processing and while in transit. [8]
- **Member State**: in these guidelines, "member State" refers to the authority in charge of regulating, conducting, or supervising the electoral process in question. Usually, but not always, it refers to the electoral management body at local, regional, or central level. It may also refer to other public institutions such as the parliament or the government.
- **Minimum level (to which legal principles should be ensured)**: it is often not possible to ensure the full respect of all principles because there might be conflicting or competing principles, such as secrecy and data protection on one side and transparency on the other. In these cases, a balance of interest must be reached and the minimum level, to which each of the conflicting principles should be ensured, needs to be defined. This decision should be taken by the competent authority, usually the legislator. The essence of the principles cannot be violated.

- **Reliability**: the ability of a system or component to function under stated conditions for a specified period of time.[9]
- **(Technical) Requirement**: a condition or capability that must be met or possessed by a system or system element to satisfy a contract, standard, specification or other formally imposed documents.[10]
- **(Legal) Requirement**: a legal requirement is a concretisation of a legal principle. For instance, the legal requirements that apply to the transmission of results from polling stations to a central election commission (for example, requirements for deadlines, formats, or checks) are derived from and are a concretisation of the principles of universal, equal, free and secret suffrage.
- **Risk**: the level of impact on organisational operations (including mission, functions, image, or reputation), organisational assets or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.[11]
- **Threat:** Any circumstance or event with the potential to harm an electoral ICT system through unauthorised access, destruction, disclosure, modification of data, and/or denial of service.
- **Usability**: usability is about designing products to be effective, efficient, and satisfying. It includes user experience design and is closely related to accessibility.[12]

---

[1]. Code of good practice in electoral matters (CDL-AD(2002)023rev2-cor), adopted by the Venice Commission at its 52nd session (Venice, 18-19 October 2002).

[2]. www.iso.org/standard/52075.html.

[3]. Definition taken from: www.w3.org/WAI/fundamentals/accessibility-usability-inclusion/.

[4]. Definition taken from: https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf

[5]. Definition taken from: https://csrc.nist.gov/glossary/term/authenticity.

[6]. Definition taken from: https://csrc.nist.gov/glossary/term/availability.

[7]. Definition taken from: www.w3.org/WAI/redesign/ucd.

[8]. Definition taken from: https://csrc.nist.gov/glossary/term/data_integrity.

[9]. Definition taken from: https://csrc.nist.gov/glossary/term/reliability.

[10]. Definition taken from: https://csrc.nist.gov/glossary/term/requirement.

[11]. Definition taken from: https://csrc.nist.gov/glossary/term/risk.

[12]. Definition taken from: www.w3.org/WAI/fundamentals/accessibility-usability-inclusion/.

Related documents
1424th meeting of the Ministers' Deputies (9-10 February 202... **17/11/2021**
www.coe.int/.../february-2022?p_p_id=101_INSTANCE_FJJuJash2rEF&...