COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 7 April 2021

CDDG(2021)6
Item 3.1.2 of the agenda

EUROPEAN COMMITTEE ON DEMOCRACY AND GOVERNANCE (CDDG)

DRAFT COMMITTEE OF MINISTERS' GUIDELINES ON USE OF ICT IN ELECTORAL PROCESSES IN COUNCIL OF EUROPE MEMBER STATES

FIRST PROPOSAL

Secretariat Memorandum
prepared by the
Directorate General of Democracy
Democratic Governance Division

Introduction

In the biennium 2020-2021, the European Committee on Democracy and Governance (CDDG) has been instructed to develop "standards on new technologies and the different stages of the electoral process (including voter registration, transmission and tabulation of results, etc.) in the form of a Committee of Ministers' recommendation or guidelines" (task ii).

To carry out the relevant preparatory work, the CDDG has set up the working group on Democracy and Technology (GT-DT). At its 12th plenary meeting, the CDDG also expressed a clear preference for the preparation of Committee of Ministers' Guidelines rather than a recommendation.

A questionnaire has been sent out with a view to collecting information. The replies to the questionnaire are compiled in the addendum to the present document, which were discussed by GT-DT at its meeting of 8 February 2021. At the same meeting, GT-DT welcomed two new expert consultants who will support the work on task ii): Mr Robert Krimmer, ERA-Chair Full Professorship of e-Governance, Skytte Institute, University of Tartu, Estonia and Ms Melanie Volkamer, Karlsruhe Institute of Technology, Germany. They join Ms Ardita Driza Maurer, legal expert, Switzerland who has been involved in this work since the beginning.

In the discussion which took place on 8 February, members of GT-DT welcomed taking an inclusive and multi-disciplinary approach stressing that the guidelines should be technology neutral and focus on principles, namely accessibility / usability, security and data protection. Furthermore, the guidelines should address questions of risk incidence and management, as well as the provision of capacity-building for civil servants. Additional issues to be considered included multilevel governance and the role and responsibilities of private companies.

The working group agreed that the Secretariat would work closely with the experts to develop a skeleton structure for the guidelines to be presented to the CDDG. The Guidelines on the implementation of the provisions of Recommendation (2017)5 on standards for e-voting could provide inspiration for that structure. Subsequently, the Bureau of the CDDG supported the proposal that GT-DT hold an online consultation on the draft Guidelines in May 2021, with the participation of the Venice Commission and Election Management Bodies (EMBs).

Action required

The CDDG is invited to discuss the structure of the draft Guidelines and to provide further guidance for this work. It is also invited to support holding an online consultation on the draft Guidelines in May 2021, and to reach out to Election Management Bodies to encourage their participation.

PROPOSED STRUCTURE FOR THE DRAFT COMMITTEE OF MINISTERS' GUIDELINES ON USE OF ICT IN ELECTORAL PROCESSES IN COUNCIL OF EUROPE MEMBER STATES

Introduction

The aim of this document is to identify elements that may feed into the future Committee of Ministers' Guidelines on the use of Information and Communication Technologies (ICT) in electoral processes. It provides the main structure for the Guidelines, describing factual situations and asking a number of questions to be addressed in the continuation of the work.

The team of experts conducted a first analysis of the current use of ICT in electoral processes in Council of Europe member States, based on the answers provided by 23 countries to the CDDG questionnaire on use of ICT in the different stages of the electoral process, and reflecting the situation as of January 2021.

Structure
Preamble
Scope of the Guidelines
Core principles
Guidelines applicable to all stages of the electoral process (1-13)
Guidelines applicable to specific stages of the electoral process (A—N)
Guidelines applicable to the use of specific technologies (O-Q)
Glossary of the terms used in the Guidelines

Preamble

Free and fair elections are the cornerstone of representative democracy. The integrity of the electoral process is fundamental to ensure that people trust democratic institutions and recognise their legitimacy.

There is a trend towards the increasing recourse to ICT in all spheres of life, including in electoral administration. **The draft Guidelines aim at contributing to ensuring the integrity of the electoral process and therefore enhancing citizens' trust in democracy by identifying safeguards and requirements to be introduced in the legislation and/or regulations of Council of Europe member States when using ICT in different stages of the electoral process**.

The draft Guidelines are inspired by relevant international obligations, recommendations and standards, including electoral and ICT related ones, by research and by good practice identified in member States.

Scope of the draft Guidelines

The draft Guidelines cover the use of ICT by the authorities in the different stages of electoral processes, with some exceptions. The use of ICT by other actors in the context of the electoral process (for instance, political microtargeting by political parties, spreading of information by media outlets) is not covered. Likewise, e-voting and e-counting as defined in the CM/Rec(2017)5 on standards for e-voting are not covered. In other words, the use of electronic means to cast and/or count the vote are dealt with in the mentioned recommendation and are not covered by the present draft Guidelines. However, hybrid forms of counting, which make use of some ICT but do not fall within the definition of e-voting according to Rec(2017)5, are covered by the present draft Guidelines.

Core principles

The use of ICT, like the use of any other technology in electoral processes, should comply with all principles of democratic elections and referendums.

Democratic elections and referendums should be held in accordance with certain principles that lend them their democratic status. The 2002 adopted Code of Good Practice in Electoral Matters[i] of the European Commission for Democracy through Law (Venice Commission), is the reference document of the Council of Europe in the field. It defines the "European Electoral Heritage" through two aspects: the hard-core 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 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 or nationality;
- *Equal suffrage:* each voter has the same number of votes, each vote has the same weight and equality of opportunity has to be ensured;
- *Free suffrage:* the voter has the right to form and to express his/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 circulation, freedom of assembly, 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 in the constitution or at a level higher than ordinary law;
- *Procedural guarantees:* these include procedural safeguards aiming at ensuring the organisation of elections by an impartial body, the observation of elections by national and international observers, an effective system of appeal among others;
- *Electoral system:* within the respect of the above-mentioned principles, any electoral system may be chosen.

General guidelines applicable to all stages of the electoral process

Countries increasingly use ICT solutions in handling electoral data and processes. Additionally, use of ICT is considered in relation to specific situations, like a pandemic, whose occurrence can make the conduct of electoral processes difficult or impossible. E-data and e-processes may improve the exercise of political rights by offering better accessibility and interaction possibilities, transparency, etc., and may procure some advantages, namely of speed, efficiency, accuracy, to election administration. At the same time use of ICT also increases complexity and exposure to threats and risks inherent to the ICT employed.

In the following, "Member State" refers to the competent authority, usually the electoral management body, which is in charge of the ICT solution used in the electoral process.

Member States shall ensure that ICT solutions respect all principles of democratic elections and referendums and shall develop requirements that fully reflect the principles.

General legal principles and requirements that apply to the different phases of the electoral process should be identified and detailed and exhaustive requirements that address use of ICT in a legally compliant way should be derived from them. Identifying the general legal requirements is a challenging task as they are not clearly stated and may need to be identified through interpretation. In doing so, due account should be taken of the specificities of the technology envisaged, namely the threats, risks and opportunities that come with each technology. The objective of all regulation is to ensure respect of political and other fundamental rights at stake in an election.

In each e-procedure or e-document, several electoral rights are involved. E-electors' registers and their online publication are relevant in ensuring the right to participate in elections, the right to consult registers and check their accuracy, etc. Candidates' registers are relevant in ensuring the right of being elected, and so on. Regulation of ICT solutions should ensure that relevant rights are implemented and respected. It should furthermore address possible irregularities, complaints and dispute resolution mechanisms related to the use of such ICT solutions.

Member States shall ensure the usability and accessibility of ICT solutions in use in the electoral process

Definition of ensuring usability and accessibility (to be drafted).

Usability should be considered from at least the perspective of the end user of the service and the perspective of the electoral staff that operates, maintains, controls etc. the solution. Usability influences the secure use of the ICT solution.

Member states shall ensure the integrity of the information provided by ICT solutions that are used in the electoral process. Procedures are put in place to detect and correct errors or any unauthorized manipulation of information.

Any change or error in the e-process or e-document can be detected and corrected**.** The possibility to detect and correct errors or manipulations is particularly important with respect to results transmission from polling station to a regional or central authority, especially if transmission is done via internet. Stakeholders shall be able to verify that the transmission was done correctly. Detected changes and errors can be corrected using the existing material (ballots, records, etc.).

Possible questions to be dealt by the regulator include the following: do involved stakeholders have the possibility to detect changes or errors introduced by ICT? Do they have the possibility to contest detected changes or errors? What are the possibilities for rectifying, etc.?

Guideline on authenticity (to be drafted)

The ICT solution shall present authentic information. The source of the information/data shall be authenticated.

Guideline on availability/reliability (to be drafted)

The underlying process / document should remain available to the stakeholders even in case of failures or attacks on the ICT solution. The data collected via the ICT solution should remain available even if the ICT solution is disrupted. How to ensure these?

Guideline on confidentiality and data protection (to be drafted)

Provisions on data protection shall be respected. To be noticed, several relevant data and processes are public and all information is published. Several electoral data, however, are sensitive and subject to stricter requirements (e.g. of confidentiality) than data protection ones. Such requirements should be provided for in the electoral legislation.

Guideline on transparency and observation (to be drafted)

Informing stakeholders concerned about the ICT solution.

Allowing observers/parties' proxies to observe ICT solutions used in elections; provide access to information about controls of ICT solutions; provide access to the source code of ICT solutions?

Maintaining analogue processes in parallel to e-backed ones (to be drafted)

Universal suffrage implies that all electoral stakeholders can accomplish all tasks and exercise all rights as foreseen by law. Maintaining parallel analogue equivalent procedures may be necessary to ensure that all stakeholders are able to do so and that no digital divide is created.

Maintaining analogue processes is foreseen for instance in countries with a strategy that tends towards digital by default.

Regulation should clarify the legal value of results produced by e-backed solutions when these are used in parallel with manual, paper-based solutions. The two can be complementary or can have different roles and values. For instance, some states foresee use of ICT only to assist the administration, excluding use of ICT for final, legally binding results.

Guideline on controls and security of the ICT solution (to be drafted)

Guideline on risk assessment and risk management (to be drafted)

Processes other than e-voting, which are important for the correct holding of an election and its correct outcome, may face risks similar to e-voting especially if the underlying solution is web-based. These should be addressed. Questions dealt with in Rec. (2017)5 like risk assessment and risk management, accountability, distribution of responsibilities, transparency and observation, reliability and security, handling of sensitive data, data standards and interoperability, are relevant to all digitisation.

Recourse to ICT solutions in emergency contexts (to be drafted considering the recent work of the Venice Commission)

Guideline on public-private partnership in implementing ICT solutions in the electoral process (to be drafted)

Safeguards to be introduced as regards outsourcing and procurement. Need to ensure in-house expertise of electoral management bodies.

Guideline on responsibility (to be drafted)

The electoral management body shall be ultimately responsible…

Guidelines applicable to specific stages of the electoral process

E-registers and e-registering

There exist several e-registers, namely of electors, parties, candidates and their financial disclosures, observers, political parties' proxies, media, translators, polling staff, etc. Some are drawn from other (e-)registers. This is the case with the electors' register, usually drawn from the civil register in countries that have them. Others are created based on an application to register. A voter may register to vote or may register to change her polling station, to ask for a special voting method like postal voting, etc.

Application to register and registering may be done online. Applications to register are followed by some control and decision-making procedure which may be e-backed and partially or totally automatised.

Guideline on ensuring unique identification/authentication of applicants (to be drafted)?

Requirements on use of eID-s, biometrics, social security numbers and other solutions for authentication purposes? Requirements for ensuring control of a person's right to interact with the system? A person may have many roles, e.g. as a voter, as a candidate, as a proxy for a party or an NGO, etc.

Furthermore, e-registers should follow the general guidelines. They are expected to contain accurate information, to protect confidentiality/secrecy of information to the extent required by law and to resist to unauthorized manipulation. The required level of confidentiality or secrecy is defined by law. The implementation of confidentiality/secrecy requirements as well as security requirements for e-registers and e-registering should be foreseen in the regulation. Transparency is necessary for verification purposes. Correction possibilities should be foreseen. Maintaining an analogue possibility of registering in addition to the online registering appears necessary to ensure universal access, at least for registers of physical persons…

E-signing

Online submission and collection of e-signatures in support of issues (initiative or referendum), candidates, a new party, etc. and their electronic processing (e.g. control of validity of signatures) is already reality in several countries and is planned in some others.

One person can sign several proposals: an initiative, a referendum demand, in support of a new party, in support of a candidate or list of candidates, etc. However, he/she should sign only once under each proposal.

Guideline on ensuring unique identification/authentication of signatories (to be drafted)?

Which e-signature is accepted for what purpose and at which level (local, national, supra-national)? Requirements on checking signatory's rights?

Furthermore, e-signing should follow the general guidelines. Requirements on the integrity of data and procedures, on confidentiality of e-signatory data, as required by law, during all steps of the process, including those on archiving and/or destroying e-signatures need clarification.

E-publication of election information

In addition to registers, several other election-related data are published online, for information purposes. Possible issues include accuracy, authenticity (information is issued by the authorized body) and integrity (protection from unauthorized manipulation).

Guideline on ensuring that information is authentic and adequately protected from unauthorized manipulation? *(this may be part of the general guideline on authenticity)*

Countries are developing good practices (e.g. digital imprints) that address the authenticity issue and offer transparency about the source of a document.

E-transmission of data between members states

Exchange of electoral registers between member states. This is necessary when voting/electing at the supra-national (e.g. European Parliament) level.

Guideline on data exchange platforms and solutions (to be drafted)?

To ensure integrity, electoral registers are exchanged through secure electronic exchange platforms.

Guideline on using/ archiving/destroying documents received from another country (to be drafted)?

E-transmission of data between central, regional and local election authorities

An Election Management System (EMS) may have several subsystems dedicated to e.g. managing voters, candidates, polling stations, local election commissions, voting results, political party financing, observers, media, etc. Central, regional and local election authorities may exchange electronic documents at all stages of an election/vote. For example, lists of voters, lists of accredited observers and media are transmitted to polling stations; a local authority may design and order local ballots using the EMS, etc.

E-backed voter authentication may be done in a centralised way. Identity information collected electronically at the polling station (including biometric information where this is collected) is transmitted ongoing to a central database which communicates with all polling stations. This solution allows the voter to vote wherever she prefers and, at the same time, enables the election authority to ensure that a voter only votes once. Based on this networking, the polling station may allow/refuse a voter to vote and motivate its decision. The centralised control of voters' authentication requires reliable connections and an exchange platform/solution. What are the requirements, including security ones, for the functioning of important registers in a country-wide network during voting day? How to strengthen polling station procedures' resilience in front of problems in the network that may occur on voting day? How to handle dependence on the network given the time constraints during voting day?

Guideline on data exchange platforms and solutions (to be drafted)?

E-training and e-accreditation

Online training of election staff and stakeholders (observers, media, voters, etc.) has gained momentum in the current pandemic context.

Specific guideline?

E-backed voter authentication (polling station)

Use of e-backed devices to read the Machine-Readable Zone (MRZ) of identity documents for the purpose of identifying voters and registering their participation. Additionally, in a few Council of Europe member States biometric data are collected (or such collection is envisaged) from voters in polling stations to make sure the person present at the polling station is the legitimate voter he/she claims to be.

Specific guideline about handling errors or alleged errors, failures, etc.?

E-registration of the voter's participation

Voter's participation in the election may be registered in an e-poll book. The e-poll book may be part of an electronic journal which contains all important figures and events about the election. Such ICT solutions may be connected to a central EMS at some point during the electoral process.

Same guideline as for authentication and transmission of data to a central authority (above)?

E-backed local processing of results

Results entry, counting and tabulation may be backed by ICT solutions. ICT tools may have embedded checks for identifying incorrect entries or arithmetical errors in counting; they flag mismatches and may be designed not to allow for data transmission before the flagged issues are addressed. Clarify the related procedures: Is it possible for the election administration to ignore flagging of possible irregularities? Should such decision be motivated?

Specific guideline?

E-transmission, consolidation, verification and publication of results

Voting results and statistics on participation, both preliminary and final ones, are regularly published. Ongoing publication of preliminary results is often conceived as a control tool allowing stakeholders to monitor and react to any possible unauthorized change. Consolidation of results, seat calculation, reports etc. are e-backed in most cases.

What is the legal value of the ICT solution used: is it conceived as a facilitator (speeding up the establishment of results) or as a control (checking the accuracy of reported results) tool? Or both? What is the legal value of the results obtained through ICT as opposed to manual ones? What are the ensuing rights and obligations?

Specific guideline?

E-submission of claims and appeals

In some countries, dispute resolution mechanisms may be accessed online, throughout the electoral process. E-backed solutions may assist authorities to handle claims, appeals, etc.

Specific guideline?

Post-election obligations

Destruction, archiving, etc. of e-data.should be foreseen in regulation.

Specific guideline?

Guidelines relating to the use of specific technologies

Cloud

The cloud is increasingly being used to host election-relevant documents and events.

Several questions can be asked in relation to the public or private cloud and their implications on electoral documents and processes ; possible requirement about maintaining in house hosting capacities (in order to keep the upper hand on election administration); the protection of sensitive data, the security of sensitive documents and processes and accountability issues on the cloud; whether the cloud introduces new vulnerabilities (e.g. to security, secrecy and privacy, interoperability) and new threats; whether forensics and investigation of irregularities become more complex; whether interoperability (and thus the possibility to take back the data and transfer it) become more complex, thus creating or increasing dependencies, etc.

Specific guideline?

Biometrics

There is currently little use of biometrics amongst Council of Europe member States even if recourse to it is being discussed in some countries.

Several questions can be asked in relation to the uniqueness and permanence of biometrical characteristics to ensure the right to vote over time; facility and speed of collecting the biometrical information and authenticating the voter on voting day; acceptability of the collection and use of biometrical characteristics by voters; security of data storage and, more generally, about system security, etc.

Specific guideline?

Blockchain

A few countries use blockchain-based ICT solutions in the electoral process.

Several questions can be asked in relation to vote secrecy (data posted on the blockchain stays there); non-publication of intermediary results (the number of votes for each candidate is known before the voting is finished); user-friendliness (important waiting times until a transaction or vote is concluded) ; respect of one-voter-one-vote principle (as computational power is important for decision-taking in this context); security, etc.

Specific guideline?

Glossary of the terms used in the draft Guidelines

ICT covers products and processes that store, retrieve, manipulate, transmit, or receive information electronically in a digital form.[ii]

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

[ii] Based on a definition by https://en.wikipedia.org/wiki/Information_and_communications_technology