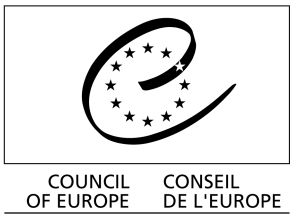
DIRECTORATE GENERAL OF DEMOCRACY AND POLITICAL AFFAIRS

DIRECTORATE OF DEMOCRATIC INSTITUTIONS

PROJECT "GOOD GOVERNANCE IN THE INFORMATION SOCIETY"



GGIS (2010) 5 fin. E

Strasbourg, 16 February 2011

Guidelines on transparency of e-enabled elections

prepared by the Secretariat

Introduction

In 2004 the Committee of Ministers of the Council of Europe adopted Recommendation (2004)11 on legal, operational and technical standards for e-voting. Following this, Council of Europe member states agreed to hold biennial meetings in order to keep under review their policies and experience of e-voting since the adoption of this Recommendation. The first such meeting took place in Strasbourg in November 2006, the second one in Madrid, Spain, in October 2008, and the third one in Strasbourg in November 2010.

At the 2008 Biennial Review meeting, the Secretariat was invited to investigate issues that could be examined in order to strengthen the implementation of the Recommendation. In particular, it was suggested that certain aspects of the Recommendation, such as the certification of e-voting systems and the transparency of e-enabled elections, required further consideration.

In recent years it has become clear that an e-voting system can only be introduced if voters have trust and confidence in their current electoral system. If such trust exists, voters are then very likely to have confidence in new e-enabled elections. However, trust should not be taken for granted and states need to do their utmost in order to ensure that it is preserved. All the more so because once trust and public confidence is diminished, it is exceedingly challenging to regain it.

Fostering transparent practices in member states is a key element for building public trust and confidence. Being transparent about the e-voting system, the processes surrounding different electoral procedures and the reasons for introducing e-voting will contribute to voters' knowledge and understanding, thereby generating trust and public confidence.

Although transparency, through the availability of documents to voters and stakeholders, is important, it will not be possible for everybody to understand an e-voting system. In order to have confidence in the electoral process, voters rely on others who are in a position to understand the materials and the processes. It is therefore essential that stakeholders have as much access as possible to relevant documents, meetings, activities etc. Acting in a transparent manner towards these specific and important groups will boost public trust and confidence because without transparency states cannot guarantee that an e-enabled election was conducted according to the democratic principles of free and fair elections.

With this in mind, review work was undertaken on the transparency of e-enabled elections. The guidelines presented in this document have been elaborated in the light of the findings and conclusions of the workshops on transparency of e-enabled elections held on 18 and 19 March 2010 in Oslo (Norway) in cooperation with the Norwegian Ministry of Local Government and Regional Development and at the Fourth International Conference on Electronic Voting, Bregenz (Austria) on 21 July 2010. They were considered and endorsed at the 3rd biennial intergovernmental meeting to review developments in the field of e-voting and the application of CM Recommendation

(2004)11, held in Strasbourg on 16-17 November 2010. The present final version of the Guidelines takes into account the comments made at that meeting.

The guidelines provide a practical tool to facilitate the implementation of the 2004 Recommendation, especially Recommendations 20 to 23 which invite member states to ensure the transparency of their voting system thereby fostering voters' and observers' confidence in the system. The Recommendations propose minimum requirements for the transparency of e-enabled elections of political elections and referendums at all tiers of governance.

OSCE/ODIHR, the leading international organisation on observation of elections, was much involved in the process of drafting these guidelines. They welcomed the cooperation with the Council of Europe to come to guidelines which focus on different ways for governments to make e-voting as transparent as possible, which should assist the observers of OSCE/ODIHR in the performance of their duties.

These guidelines do not intend to prescribe a particular system or to impose specific processes on a country, but rather they offer objective tools and provide member states with guidance on how to optimise transparency thereby helping them to improve their current processes and exchange information on best practises.

The Guidelines address relevant aspects relating to all stages of elections and referendums, i.e. the pre-voting stage, the casting of the vote, and the post-voting stage, as well as to the roles and responsibilities of different stakeholders. Not every government will use electronic means in all aspects of elections; hence these guidelines are applicable to those stages in which member states decided to use electronic means.

The guidelines laid out in this document are each followed by explanatory paragraphs. A glossary of relevant terms is provided in Appendix I and relevant extracts from Recommendation (2004)11 can be found in Appendix II.

GENERAL

1. Member states should only introduce an e-voting system if public trust in the current electoral system exists

Before any e-voting system is introduced it should be clear that a substantial majority of the public has enough confidence in the existing electoral system. Public trust and also political trust such as confidence in parliament is essential for the successful implementation of e-voting. Without such confidence and trust, there is a potential for political and public unrest. Public trust can be fostered through transparency and openness of all aspects of the electoral system and by implementing the various recommendations and guidelines which have been developed by international organisations such as the Council of Europe and OSCE/ODIHR.

Openness is only one dimension of trust. Trust is a multidimensional issue and can therefore also be generated through other means. For example, member states should take adequate time and opportunity to also organise public debates or public consultations, which can be binding or not. A second example is to have a broad consultation with groups representing people with disabilities or other special needs. By having a dialogue with the citizens to find out their opinion and their preferences, trust can be created and/or kept.

Besides general public trust, the citizens also need to have confidence that those who are responsible and those who are involved in the organisation of an electronic election are trustworthy. These include the team which organises the elections, the poll workers, the vendors and the accreditation and certification bodies.

Having or creating a trustworthy environment does not mean there is no room for critical questions to be asked. It is important to create platforms for criticism by for example inviting NGOs to participate in the debate. However, this all needs to be done in reasonable ways. Governments are not responsible for organising their own opposition, only for the facilitation.

Some people argue that the introduction of e-voting can also boost public confidence in elections where it does not exist. However, building or boosting public trust should never be the primordial reason to introduce e-voting.

2. Member states should be as transparent as possible in all aspects of e-enabled elections

Transparency can be achieved by being open about for example the notification of elections, registration procedures, nomination of candidates, voting procedure,

publishing and explaining the results and procedures for complaints about the electoral process. Member states should not only focus on the electronic voting system and the voting stage itself, but should also ensure transparency regarding all the procedures before, during and after Election Day, providing they are a feature of e-voting. It should be stressed that such transparency should cover all voting channels whether it being remote e-voting or e-voting in a polling station. This can for example be done by showing videos on the official website in which the important facts concerning the election are explained and which especially demonstrate the voting process. The use of sign language and subtitles in these videos should also be included to further reduce barriers.

Federations of people with disabilities should be involved in the process of introducing e-enabled elections so as to see how this could affect the people they represent.

Member states regulate who has access to what and when and under what circumstances to the e-voting system.

3. When introducing e-voting, member states should clearly explain the benefits and value-added of an e-voting system

Member states can build voter confidence by being transparent about the reasons behind the proposal to introduce electronic features in the electoral process. The worries voters may have such as the safety of their vote, user friendliness, and possible difficulties with voting should be addressed in this explanation. Changing the voting system without addressing the voters' concerns should not be acceptable to other stakeholders.

LEGAL MATTERS

4. Before introducing an e-voting system, member states should analyse changes required to the relevant legal framework

A new voting system may in all likelihood require changes to the existing legal framework. Before introducing electronic voting, member states should have reviewed and secured all the legal matters in order to avoid conflicts during the process of an e-enabled election. It is also important that member states explain why certain changes to legislation are required. This will also reinforce voters' and other stakeholders' trust and confidence.

In addition to electoral legislation, regulations and codes of conduct should also be reviewed. Criminal legislation and civil laws may also require modification as new voting methods could, for example, lead to new fraudulent practices.

5. Provisions need to be made for domestic and international observers

If there is a legal provision for election observation in place, the introduction of e-voting calls for its review. For the observation of e-voting, legislation should stipulate procedures that should be sufficient for making effective observation. This might include a presence in polling stations and/or data transfer and data processing sites as well as access to documentation and reports, access to testing, audit and evaluation procedures as well as access to persons who performed these tests, audits and evaluations. In some countries, this access could be defined through regulation rather than law. One also has to be aware of the fact that new e-voting technologies might require novel observation methods in order to reach meaningful conclusions.

Member states may also wish to regulate observer access in order to manage the impact on election officials and others during the pre-election period. Accreditation is a common means of regulating observer access. This could include requiring observer groups to adhere to a code of conduct such as the one developed in the 2005 Declaration of Principles for International Election Observation[1]. The methodology of accreditation should be publicly available.

Provisions should also be made for long term domestic observers. The introduction of e-voting should be accompanied by local observers such as independent electoral commissions and local NGOs. Member states should act as transparently as possible towards these groups.

ACCESS TO DOCUMENTATION AND REPORTS

6. Domestic and international observers require access to all relevant documentation on e-voting processes

Access to documentation including minutes, certification, testing and audit reports as well as detailed system's documentation explaining in details the operation of the system, is essential for domestic and international observers. They should be

[1]These guidelines were established by the United Nations and endorsed by African Union, Asian Network for Free Elections (ANFREL), The Carter Center, Center for Electoral, Promotion and Assistance (CAPEL), Commonwealth Secretariat, Council of Europe European Commission for Democracy through Law (Venice Commission), Council of Europe – , Parliamentary Assembly, Electoral Institute of Southern Africa (EISA), European Commission, European Network of Election Monitoring Organizations, (ENEMO), Electoral Reform International Services (ERIS), IFES, International IDEA, Inter-Parliamentary Union, International Republican Institute (IRI), National Democratic Institute (NDI), Organization of American States (OAS), Organization for Security and Cooperation in Europe, Office of Democratic Institutions and Human Rights (OSCE/ODIHR), Pacific Islands, Australia & New Zealand, Electoral Administrators' Association (PIANZEA), Pacific Island Forum, United Nations Secretariat.

invited to relevant meetings. Where possible, member states, the vendor or the certification body should provide information to all stakeholders, for example by posting relevant documents on the internet well in advance of the election period.

As mentioned in guideline number 2, member states should develop procedures in which it is defined who has access to what and when. Such procedures should also be developed for domestic and international observers as well as for the media. Also procedures for other stakeholders such as citizens, political parties and NGOs need to be established. Open Access should be the central theme in these procedures.

Member states should make these requirements clear to potential vendors who should also understand that stakeholders, and specifically domestic and international observers, require access to certain documentation during the tender process. Non-disclosure agreements, which prevent observers from publishing assessments, and the facts on which assessments are based, would withhold important information from all stakeholders, but most importantly from observers.

7. Member states should make the relevant documentation available to stakeholders well in advance of the pre-election period

Review of the necessary documentation should take place well before the immediate pre-voting period. If accreditation is required in order to access e-voting documentation, bodies (including domestic and international observers) should be able to obtain accreditation well in advance.

8. Member states should make the relevant documentation available to observers including, as far as practicable, in a language commonly used in international relations

Relevant information required by domestic and international observers to carry out their work satisfactorily should be available in the official language, or languages, of the country concerned. Such information should, as far as possible, also be made available in one of the official languages of the Council of Europe (English and French). In particular international observers require access to documentation in one of these languages.

TESTING

9. Domestic and international observers and the media should be able to observe the testing of the software and hardware

Stakeholders, including accredited observer groups, should not only have access to documents, but should also be able to observe the verification of the e-voting devices/system. The observation of such tests and/or audits should not be allowed to interfere with the conduct of the election; therefore such monitoring should only take place under guidance of those who are responsible for the organisation of elections. Furthermore, the people conducting the observation of the tests and/or audits should attend a training session in advance. The process should be open enough to allow observers to have full insight into the operation of the device.

TRAINING

10. Member states should provide training programmes for domestic and international observer groups

E-voting systems are not easily understandable for non-experts. In order to improve stakeholders' appreciation of the system in use, training is necessary, in particular for domestic, but also for international observers. It should provide basic and easy tools for use in observation work. This would include ways to check seals, read a voting machine print out and read an audit file.

SYSTEM

11. Member states should take appropriate steps to avoid circumstances where the election is dependent on a few major vendors

Software and hardware of an e-voting system require ongoing maintenance. This is in addition to the procedures required for a specific event, for example the creation of ballot papers. It is important for member states not to be over dependent on just one or two vendors for all of these actions since this could result in a vendor-lock-in. If considering outsourcing, it is essential that those who are responsible for the elections understand what is being outsourced, why it is being outsourced and what methods and processes the vendor intends to undertake. Statutory duties of the body responsible for the conduct of elections must never be outsourced, since this body is in charge of the election.

12. Member states should consider the voting source code as part of the measures to allow for universal auditability

To ensure public confidence and follow the principle of transparency and reproducibility, the voting software source code, the configuration as well as the list of all hardware and software components of the e-voting system (see also Rec (2004)11, paragraph 69) should be part of the audit trail that has to be archived according to local law.

Furthermore, protocols of audited processes such as the installation and setup procedure, the verification that the certified source code is the one used during the election, and the tallying process of the electronic ballot sheets should also be part of the audit trail. This should help member states to provide relevant documentation to third parties, including national and international observers and media, thereby reinforcing transparency about the system and its processes.

13. When applying e-voting in polling stations, member states should consider the use of a second medium to store the vote to improve transparency

Besides the primary electronic storage of the cast vote, it is recommended to have a second paper or "software independent" medium to store the vote in order for the voter to verify his vote and which can be used for a manual recount if necessary, and for audit purposes. It can also be used as a potential backup in case the voting computer breaks down or fails in another area. One of the reasons for introducing this second medium is to reinforce people's trust in the system. It should provide physical, unalterable evidence of how the voting computers interpreted the voter's vote. However, usage of the second medium must not compromise the privacy of vote casting.

The most common example of storing the cast vote on a second medium which is currently used is the Voter Verified Paper Audit Trail (VVPAT). A device that produces a paper trail can be added to voting computers in a polling station. The voter would cast his/her vote on the computer and a printed version of the vote would either be shown to the voter behind a glass screen or given to him/her who would then put the printed version of the vote in a ballot box. This latter option has the problem that the printed version could, accidentally or not, disappear which could potentially lead to vote selling or to the option that the voter has to show proof of how he/she voted, which could lead to undue pressure on the voter.

Member states should, however, be aware that it is also a costly system and a source of potential failures. For example, what to do if a printer fails or runs out of ink and thus canno longer a printout of the vote?

A paper trail which reveals the content of the vote should not be added to the voting tools in uncontrolled areas like from home since this could lead to "vote selling".

A solution to this issue could be 'end-to-end verification'. Such systems often use cryptographic methods to create receipts that allow voters to verify after the election that their votes were not modified, without revealing which candidates were voted for. Voters would then for example, after they have cast their vote, receive a digital code. After the election, voters may then go to a website and verify through that code if his or her vote has been counted.

Another solution could be the 'reversible vote'. A voter may cast his or her vote via the internet as many times as he or she wishes and on Election Day he or she may go to the polling station. The vote which will be counted is either the last vote cast via the internet, or the vote cast in the polling station. In this way it is useless to buy votes because the voter can always change his or her vote back to what he or she wishes to vote.

Another example is the storage of the vote as a PDF file on a smartcard. If required, such PDF files can be printed so as to enable a paper ballot count.

Member states should explain to the general public why they use this second medium, how it will be used and for what. Likewise, member states should also explain to the general public if they decide not to use it.

14. If during an e-enabled election in polling stations where the vote is also stored on a second medium, a mandatory count of the second medium in a statistically meaningful number of randomly selected polling stations should be carried out

In order to foster trust in the process, a mandatory count of this second medium in a statistically meaningful number of randomly selected polling stations should be carried out. However, it is important that polling station officials are not informed in advance about the polling stations in which this extra count will be carried out.

15. Member states should develop rules dealing with discrepancies between the mandatory count of the second medium and the official electronic results

When member states use a second medium to store the vote and a mandatory count is carried out, discrepancies between the results of votes cast may arise. In such cases the rules should make clear which type of vote (electronic or the second medium) takes precedence. A case for electronic vote precedence is that voters have cast their vote in this manner. A case for the second medium would be

that this vote could have been verified by the voter themselves, particularly if the medium under consideration includes a paper trail.

Therefore in case of any discrepancy, the case should be examined thoroughly and any decision on the result of the vote-count should depend on the result of the investigation. Member states are asked to establish rules which should address which vote is used in the official counts, if and when a recount is considered necessary, when and how the mandatory count takes place, under which circumstances all second votes are counted, and when a re-election should be held.

16. Member states shall gain experience in providing mechanisms that allow voters to check whether their vote was counted as intended

In order to facilitate the development of the concept of chain of trust in e-enabled elections, member states should facilitate research and pilot projects in which voters should be able to verify if their vote was

- cast as intended
- recorded as cast
- counted as recorded.

Appendix I

Glossary of terms
used in the Guidelines on the transparency of e-enabled elections

In this document the following terms are used with the following meanings:[2]

Chain of trust: a process in computer security which is established by validating each component of hardware and software from the bottom up. It is intended to ensure that only trusted software and hardware can be used while still remaining flexible.

Guideline: any document that aims to streamline particular processes according to a set routine. By definition, following a guideline is never mandatory.

Open Access: access to material via the internet in such a way that the material is free for all to read, and possibly to use (or reuse) to various extents.

Stakeholder: a person, group, organisation, or system that has an impact on, or can be affected by, a government's or organisation's actions. These include citizens, election officials, political parties, domestic and international observers, media, governments, academics, (I) NGOs, anti-e-voting organisations and specific e-voting certification bodies;

Transparency: the concept of determining how and why information is conveyed through various means.

[2] For more elaborate explanations please refer to www.wikipedia.org

Appendix II

Text of Recommendation 2004 (11) on Legal, operational and technical standards on e-voting

B. Procedural safeguards

I. Transparency

20. Member states shall take steps to ensure that voters understand and have confidence in the e-voting system in use.

21. Information on the functioning of an e-voting system shall be made publicly available.

22. Voters shall be provided with an opportunity to practice any new method of e-voting before, and separately from, the moment of casting an electronic vote.

23. Any observers, to the extent permitted by law, shall be able to be present to observe and comment on the e-elections, including the establishing of the results.

Text of explanatory memorandum of Recommendation 2004 (11) on Legal, operational and technical standards on e-voting

Standard No. 20. "Member states shall take steps to ensure that ..."

55. Confidence by voters and candidates in the voting system(s) used is essential, not only to participation but also to the democratic system of the member state. Full understanding of the e-voting system(s) in use is the basis for this confidence.

56. Traditional voting methods are simple and well tried and tested in member states. Voters are familiar with voting systems using ballot papers and ballot boxes and understand the general rules that govern how they should vote and how their vote is collected and counted unaltered. The introduction of e-voting produces a new situation in which voters will be less familiar with the electoral process and perhaps less able to understand the safeguards built into the e-voting system. Accordingly, as e-voting systems are introduced, it is likely that, in order to maintain voter understanding and confidence, steps will have to be taken to introduce the system to voters. Over time, it may be necessary to continue to take such steps in order to secure the understanding and confidence of voters who are unfamiliar with e-voting.

57. Confidence can be enhanced by providing voters with as much information as possible about the method of e-voting being used.

Standard No. 22. "Voters shall be provided with an opportunity to practice ..."

58. A new e-voting system may cause voters anxieties of different kinds. In order to promote understanding and confidence in any new e-voting system, including in its transparency, opportunities to try out the system should be provided before, and separately from, the moment of casting an electronic vote. Special attention should be paid to any voters who are not familiar with the new e-voting method, for example the elderly.

Standard No. 23. "Any observers, to the extent permitted by law ..."

59. There are various international and domestic obligations on election observation: by representatives of candidates, as well as by independent domestic and/or international observers. All member states are bound to the commitments of the Document of the Copenhagen Meeting of the Conference on the Human Dimension of the OSCE of 29 June 1990 to "invite observers from any other OSCE participating state and any appropriate private institution and organisation who may wish to do so to observe the course of their national election proceedings [… and …] facilitate similar access for election proceedings held below the national level".

60. Observers should be able to verify that the e-voting system itself is designed and operated in a way which respects the fundamental principles of democratic elections and referendums. Therefore, member states should have clear legal provisions on observers' access to the e-voting system documentation and audit data.

61. E-elections/e-referendums pose special challenges to observers, inherent in the electronic method of the election or referendum. Observers will thus have to be provided with an opportunity, in particular, to have access to relevant software information, to see physical and electronic safety measures for servers, to inspect and test certified devices, to have access to and test sites and information provided for remote e-voting, and to observe cast electronic votes entering the electronic ballot box and that votes are being counted. Security measures for telephone or Internet voting may, however, make it necessary not to allow the presence of observers in the computer room itself. In that case measures should be taken in order to give the observers the opportunity to monitor the activities.