Compendium of e-voting and other ICT practices

Non-Paper from the Commission services

Compendium of e-voting and other ICT practices

Non-Paper from the Commission services

TABLE OF CONTENTS

1. Introduction

As the digitalisation of European society evolves, information and communication technology (ICT) solutions are being used increasingly in the context of electoral processes.

The European democracy action plan[1] announced the preparation of a compendium of electronic voting ('e-voting') practices by the Commission, together with Member States and in close cooperation with the Council of Europe.

In the 2020 EU Citizenship Report[2], the Commission pledged to discuss, as part of the European cooperation network on elections, practices in remote voting and specifically electronic voting (e-voting) along with online tools that can facilitate electronic democratic participation while addressing security and confidentiality concerns. The Commission strategy for the rights of people with disabilities 2021-2030 provides for the compendium of e-voting practices to address the needs of citizens people with a disabilities[3].

This compendium is designed to promote the development of a body of common knowledge among Member States on e-voting as well as the use of ICT in electoral processes[4], with the overall aim of consolidating the capacity of the competent authorities to promote high electoral standards supporting free, fair and resilient elections in the European Union, including how to address electoral threats. The compendium does not aim to provide universally applicable solutions, because the successful implementation of the of e-voting and ICT practices it cites may depend on the specific context in each Member State.

This compendium has been prepared in the context of a growing appetite for digitalisation in electoral processes[5], including the use of voting machines and internet voting, and for the use of ICT to tally votes or transmit results. The COVID-19 pandemic and the need for physical distancing have prompted renewed interest in complementary voting methods, including remote voting, which often go together with ICT solutions.

Internet voting, which allows citizens to directly submit their vote electronically from any location, is not widespread in Europe. It is being used as an option for all voters in Estonia and in some other countries such as France for voters resident abroad.

At the same time, Member States make use of ICT solutions for various purposes, for example to collect and update voter data, gather endorsement signatures for candidates, register candidates and election observers, support election administration, report on election campaign financing, and report voter turnout. Several Member States also use ICT solutions to send and

---

[1] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European democracy action plan (COM/2020/790 final).
[2] https://commission.europa.eu/system/files/2020-12/eu_citizenship_report_2020_-_empowering_citizens_and_protecting_their_rights_en.pdf
[3] Commission Strategy for the Rights of Persons with Disabilities 2021-2030.
[4] An informal subgroup of the European Cooperation Network on Elections – on e-voting – was created to allow discussions on the content of the compendium, where it was agreed that the compendium will also include ICT practices used in electoral processes.
[5] As noted by the Council of Europe in the Committee of Ministers' Guidelines on the use of ICT in electoral processes in Council of Europe Member States, there is a current trend to rely increasingly on ICTs in all walks of life, including election administration. The International Institute for Democracy and Electoral Assistance (IDEA) lists ICT that can support the conduct of each phase of the electoral cycle, during the pre-electoral and the post-electoral phases: https://www.idea.int/data-tools/data/icts-elections.

aggregate voting tallies from polling stations or counting centres to central administrative authorities, and to calculate mandates and publish results.

While bringing specific benefits, these developments in electoral processes pose different challenges, related in particular to security and voting integrity or confidentiality[6]. There are growing concerns about elections being a target for cyberattacks, such as hack-and-leak operations to gain access to voter information and interfere with the electoral process[7], or distributed denial-of-service (DDoS) attacks, preventing voters from accessing connected online voting services and websites. Possible vulnerabilities of electoral systems to manipulation, especially by malicious non-EU countries or non-state actors, have made cybersecurity one of the crucial factors for maintaining public trust in electoral processes. This must be considered before introducing e-voting or ICT in elections[8].

Organising e-voting can be a long and sometimes costly process that may require years of planning and preparation. In most cases, existing off-the-shelf e-voting solutions are tailored to non-political selection processes and do not sufficiently address the high stakes that official elections entail. Member States may develop their own solutions to fit their needs, including security requirements[9], or they can buy an off-the-shelf solution from a private supplier and take the time to adapt it to suit their needs[10].

When implementing e-voting methods and ICT in elections, Member States should build in the necessary safeguards to ensure free, fair and resilient elections that fully uphold democratic standards and fundamental rights, including data protection and cybersecurity, as the technology evolves.

This compendium contains a non-exhaustive description of existing practices in some Member States that use electronic means at different stages of the electoral process. It provides a description of e-voting solutions, such as the use of e-voting machines and internet voting, as well as other ICT solutions used in electoral processes in the EU[11]. It also presents some practices aimed at addressing the attendant risks and highlights practices that support election accessibility for people with disabilities[12]. References to compliance with data protection requirements and Council of Europe standards reflect Member States' own assessments.

---

[6] Eurobarometer data show interest in remote voting options among Europeans, although some have concerns about accessibility, data protection, potential fraud, secrecy of the vote and security of the ballot (Eurobarometer 507 on democracy in the EU). Nonetheless, it has become apparent that internet voting could become significant, including in the event of natural disasters, where internet is available, or during pandemics, as it may be key to facilitating voting when it is not possible to access certain polling stations.

[7] European Parliament resolution of 9 March 2022 on foreign interference in all democratic processes in the European Union, including disinformation: https://www.europarl.europa.eu/doceo/document/TA-9-2022-0064_EN.html.

[8] Guideline 1 of the Committee of Ministers' Guidelines on the use of information and communication technology (ICT) in electoral processes in Council of Europe Member States.

[9] Estonia, for example.

[10] In the case of internet voting for French citizens resident abroad, for instance, the software solution is chosen two years before the election.

[11] The Declaration of Principles for International Election Observation has developed general principles and guidelines for electoral ICT, offering guidance to electoral management bodies (EMBs) in countries outside the EU that are thinking of introducing ICT in their electoral processes. The general principles and guidelines for electoral ICT were adopted by the Commission's Group for External Coordination (EXCO).

[12] See also the guide of good electoral practice addressing participation of citizens with disabilities in the electoral process.

This compendium has been prepared together with Member States in the framework of the European cooperation network on elections. A dedicated subgroup of this network has been established to support discussions on this compendium.

2. Definitions

E-voting – in this compendium, e-voting should be understood as the use of electronic means for the act of voting and/or counting purposes. This covers e-voting machines in polling stations, the use of optical scanners to register and/or count paper ballots as well as remote e-voting (i.e. **internet voting**), which would occur outside the premises where voting would normally take place[13].

ICT – in this compendium, ICT refers to technology used in the electoral context such as for:

- collecting electronic signatures in support of initiatives/petitions, candidates or parties;

- publishing election-related information online;

- consulting the electoral register to check voter eligibility;

- sending election data electronically between electoral authorities;

- providing online training for election officials and other stakeholders;

- issuing electronic accreditation for observers;

- determining, processing, sending or publishing election results;

- observing different election-related activities[14].

3. Increasing interest in e-voting solutions in the EU

In 2020, following the outbreak of the COVID-19 pandemic, Member States had to accommodate voters who were not able to vote in elections in person or at their designated polling station.

A study[15] published by the Commission in July 2021 presented an overview of the legislative developments and electoral practices in remote voting in the EU Member States and explored the range of remote voting methods deployed in elections held during the COVID-19 pandemic.

The study addressed Member States' planning and implementation of remote voting methods and their organisation in the safest way possible, in the light of experience gained during the pandemic. The findings of the study included designing voting arrangements with the needs of the most vulnerable in mind so that they do not face exclusion. For instance, the study indicated that internet voting solutions should provide audio instructions for the visually impaired, and should not be overly technically challenging, in order to remain inclusive for specific groups of voters, such as older voters or people with disabilities.

---

[13] Recommendation CM/Rec(2017)5 of the Committee of Ministers to Member States on standards for e-voting (adopted by the Committee of Ministers on 14 June 2017 at the 1,289th meeting of the Ministers' Deputies).
[14] Committee of Ministers' Guidelines on the use of information and communication technology (ICT) in electoral processes in Council of Europe Member States.
[15] The Commission's Academic Network on European Citizenship Rights updated a previous 2018 'Study on the Benefits and Drawbacks of Remote Voting': https://commission.europa.eu/system/files/2022-01/eu-citzen_-_report_remote_voting_update.pdf

In September 2021, a study was prepared for the Commission[16] on the impact of new technologies on free and fair elections, concentrating primarily on how such technologies affect voters' opinions and behaviour. The study included specific recommendations of possible relevance to this compendium. These include how to facilitate the use of EU resources and encourage exchanges of experience on the use of digital solutions in the electoral context, exploring new technologies' capability to be applied in the context of elections and focusing on their reliability, trustworthiness and accountability.

Member States are discussing these topics in the European cooperation network on elections[17]. In 2022, as a follow-up to the European democracy action plan[18] the Commission started to roll out a 'joint mechanism for electoral resilience', which supports the deployment of joint expert teams and expert exchanges between Member States. This capacity-building tool is aimed at making electoral processes more resilient to various types of threat, in particular as regards online forensics, disinformation and cybersecurity during elections. The mechanism has also been used to support the work of the Commission and Member States as they prepare this compendium.

In its resolution of 26 November 2020 on a stocktaking of European elections, the European Parliament stated that new remote voting methods for citizens during European elections could improve the European electoral process[19]. On 3 May 2022, the Parliament adopted a draft legislative act proposing to repeal the Act of 20 September 1976 concerning the election of the members of the European Parliament by direct universal suffrage (Electoral Act) and replace it with a new Council Regulation on the election of the members of the European Parliament by direct universal suffrage[20], where it called on Member States '*to consider the possible introduction of complementary enhancing tools such as advance physical voting and proxy voting, as well as electronic and online voting, in accordance with their own national traditions, taking into account the Council of Europe's recommendations in those areas*'[21].

Parliament's draft legislative Act also referred to appropriate safeguards to ensure the reliability, integrity and secrecy of the vote, accessibility for people with disabilities, transparency in design and deployment of electronic and internet systems, the possibility for manual or electronic recounts without compromising the secrecy of the vote and the protection of personal data in accordance with applicable EU law.

---

[16] Study on the impact of new technologies on free and fair elections, Trasys International, September 2021: https://commission.europa.eu/system/files/2022-12/Annex%20I_LiteratureReview_20210319_clean_dsj_v3.0_a.pdf

[17] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/eu-citizenship/democracy-and-electoral-rights/european-cooperation-network-elections_en.

[18] Communication of 3 December 2020 from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Democracy Action Plan (COM/2020/790 final).

[19] European Parliament resolution of 26 November 2020 on stocktaking of European elections (2020/2088(INI).

[20] European Parliament legislative resolution of 3 May 2022 on the proposal for a Council Regulation on the election of the members of the European Parliament by direct universal suffrage, repealing Council Decision (76/787/ECSC, EEC, Euratom) and the Act concerning the election of the members of the European Parliament by direct universal suffrage annexed to that Decision (2020/2220(INL) – 2022/0902(APP)).

[21] The 2018 amendment to the Act of 1976, which did not enter into application yet, refers to the use of electronic and internet voting, while ensuring, in particular, the reliability and secrecy of the vote and the protection of personal data, in accordance with applicable EU law.

4. Regulatory context

4.1 EU level

4.1.1 Data protection

Among relevant EU law, the **General Data Protection Regulation** (GDPR)[22] is particularly important when designing e-voting rules. This is because these voting procedures often involve the automated processing of the personal data[23] of voters and candidates. In 2018, the Commission published a guidance document on the application of data protection law in the electoral context[24].

In the context of e-voting, some of the personal data processed could belong to so-called special categories of personal data under the GDPR[25], in so far as they would include, for example, biometric data which is processed for the purpose of uniquely identifying a natural person or other data revealing political opinions.

4.1.2. Cybersecurity

The **NIS2 Directive**[26] lays down, among others, cybersecurity risk-management measures for specific entities, which include entities manufacturing computer and electronic products, that could be used in elections. In addition, Member States could extend these obligations to other entities, including entities operating ICT solutions relevant for e-voting or elections.

The proposed **Cyber Resilience Act**[27] will introduce mandatory security requirements[28] for hardware and software products, including software that supports election processes. Once adopted, it could reduce the vulnerabilities of election infrastructure, including for instance the risk of election machines being leveraged by malicious cyber threat actors to interfere in elections.

Further, the **Compendium on Cyber Security of Election Technology**, endorsed by the Network and Information Systems (NIS) Cooperation Group members and published in July 2018[29], provides practical guidelines based on good practice by its contributors.

---

[22] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

[23] As a reminder, personal data are defined as 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person' (Article 4 GDPR).

[24] [2_EN_ACT_part1_v8.docx (europa.eu)](europa.eu)

[25] Article 9 GDPR.

[26] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance).

[27] [https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act#:~:text=Cyber%20Resilience%20Act%20The%20proposal%20for%20a%20regulation,to%20ensure%20more%20secure%20hardware%20and%20software%20products](https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act).

[28] Such requirements do not touch on elements specific to e-voting, e.g. the privacy, secrecy, anonymity, integrity, uniqueness and authenticity of votes.

[29] The NIS Cooperation Group comprises representatives of Member States, the Commission, and the European Union Agency for Network and Information Security.

The Commission proposal for **Artificial Intelligence Act**[30] will set harmonised rules for the development, placement on the market and use of AI systems. These could also be relevant in an electoral context.

4.1.3. Accessibility

Directive (EU) 2019/882[31] (European Accessibility Act) on the **accessibility requirements for products and services** promotes full and effective equal participation by improving access to mainstream products and services that, through their initial design or subsequent adaptation, address the particular needs of persons with disabilities. Annex I to the Directive in question lays down the specific accessibility requirements for products and services, while Annex II provides non-binding examples of practical solutions that help meet these accessibility requirements. These solutions cover the provision of information, user interface and functionality design, product packaging and instructions, service provision, and specific services all of which could also be relevant for ensuring the accessibility of e-voting solutions[32].

Directives 2014/24/EU[33] and **2014/25/EU**[34] establish that, for all procurement which is intended for use by natural persons, whether general public or staff of the contracting authority or entity, the technical specifications are, except in duly justified cases, to be drawn up so as to take into account accessibility criteria for persons with disabilities or design for all users. Furthermore, those Directives require that, where mandatory accessibility requirements are adopted by a legal act of the Union, technical specifications musy, as far as accessibility for persons with disabilities or design for all users are concerned, be established by reference thereto.

Directive (EU) 2016/2102[35] **(Web Accessibility Act)** introduces accessibility principles for the websites and mobile applications of public sector bodies, namely:

- that information and user interface components must be presentable to users in ways they can perceive;
- **operability**, meaning that user interface components and navigation must be operable;
- **understandability**, meaning that information and the operation of the user interface must be understandable;
- **robustness**, meaning that content must be robust enough to be interpreted reliably by a wide variety of users, including assistive technologies[36].

---

[30] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain EU legislative acts (COM/2021/206 final).

[31] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0882

[32] Annex 2 to the Directive provides examples of potential relevance in the context of e-voting, such as providing visual and tactile information or visual and auditory information; providing electronic files which can be read by a computer using screen readers; allowing for the use of headphones which will receive on-screen text in audio format; allowing users of an interface to enlarge a text, zoom in on a particular pictogram or increase the contrast; offering a connection with a refreshable Braille display; providing instructions by using the same wording in a consistent manner, or in a clear and logical structure, so that people with intellectual disabilities can better understand them; providing for a blind person to be able to use a file by printing it in Braille; and ensuring that technical protection measures, rights management, information or interoperability issues do not prevent the text from being read aloud by the assistive devices.

[33] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02014L0024-20220101

[34] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02014L0025-20220101

[35] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L2102

[36] Those principles of accessibility are translated into verifiable success criteria, such as those forming the basis of European standard EN 301 549 V1.1.2 'Accessibility requirements suitable for public procurement of ICT products and services in Europe' (2015-04) (European standard EN 301 549 V1.1.2 (2015-04)), via standards and a common methodology to test the conformity of content on websites and mobile applications with those principles.

4.2 International standards

Relevant international standards are designed to safeguard aspects such as voting secrecy, which includes security measures to protect against cyberattacks, including the avoidance of data leaks, the integrity of the vote, transparency, accountability, and public confidence in the process.

The **Council of Europe** has provided substantial guidance in the area of e-voting, notably through a recommendation on standards for e-voting[37], aiming to standardise the implementation of the principles of democratic elections and referendums when using e-voting, together with relevant guidelines on how to implement the recommendation [38] and an explanatory memorandum[39].

In addition, in 2022 the Council of Europe issued guidelines on the use of ICT in electoral processes in its Member States[40].

Article 29 of the United Nations Convention on the Rights of Persons with Disabilities seeks to ensure that voting procedures, facilities, and materials are appropriate, accessible and easy to understand and use, to protect the right of persons with disabilities to vote by secret ballot in elections and public referendums without intimidation, and to facilitate the use of assistive and new technologies where appropriate.

Other relevant documents in this context are the Code of Good Practice in Electoral Matters of the Venice Commission[41] and the Report on the Compatibility of Remote Voting with the Standards of the Council of Europe[42].

The work of the Council of Europe's Committee on Artificial Intelligence towards a legally binding framework on the development, design and application of artificial intelligence, is relevant in terms of the use of AI systems at different stages of the electoral process.

Article 25 of the **International Covenant on Civil and Political Rights** (ICCPR) recognises and protects the rights of every citizen to take part in the conduct of public affairs, to vote and to be elected, and to have access to public service.

5. Use of e-voting practices and other ICT in the EU

This section illustrates the use of specific e-voting machines at polling stations in Belgium and in the district of Évora, Portugal, as well as internet voting systems used in Estonia and France (for French citizens resident abroad)[43].

---

[37] Recommendation CM/Rec(2017)5 of the Committee of Ministers to Member States on standards for e-voting (adopted by the Committee of Ministers on 14 June 2017 at the 1,289th meeting of the Ministers' Deputies).

[38] Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting.

[39] Explanatory Memorandum to Recommendation CM/Rec(2017)5 of the Committee of Ministers to Member States on standards for e-voting.

[40] Committee of Ministers' Guidelines on the use of information and communication technology (ICT) in electoral processes in Council of Europe Member States.

[41] Adopted by the Venice Commission at its 52nd session, Venice, 18-19 October 2002 – https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-STD(2003)034-e

[42] Adopted by the Venice Commission at its 58th session, Venice, 12-13 March 2004 – https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2004)012-e.

Regarding other ICT solutions, the modernisation of voter registration in Ireland is mentioned, as are the use of ICT in managing complaints, notifications, and contingency reports in elections in Lithuania, the verification of voter eligibility and prevention of multiple voting in Romania, and the tabulation of election results using ICT in Czechia.

As discussed among Member States experts in the European cooperation network on elections in the context of preparing this compendium, in order to describe comprehensively the practices being used, information is provided about the relevant legal framework, the software system and technology used, the testing methodology, functional and operational flows, relevant communication campaigns (including to build voter trust and confidence), accessibility for people with disabilities, and threats and vulnerabilities identified, together with the related mitigation measures. It reflects inputs from members of the European cooperation network on elections.

A specific section concerns measures taken by Member States to support compliance with data protection requirements and in particular the GDPR.

Other international standards, including those of the Council of Europe related to the protection of electoral processes, are particularly relevant to Member States, all of which are Council of Europe members.

The issues mentioned in this compendium regarding measures being taken to ensure that e-voting or other ICT practices comply with EU law, including data protection, and international standards (in particular, the Council of Europe standards) are the result of self-evaluation by the Member States concerned.

5.1 Belgian e-voting machines

5.1.1   Short description

In Belgium, e-voting via voting machines at polling stations is available in all 19 Brussels municipalities, 159 Flemish municipalities and the nine German-speaking municipalities.

The first automated voting trial took place in Belgium during the 1991 elections in the electoral cantons of Verlaine and Waarschoot. Two systems were tested on that occasion: an electronic pen the voter could tap on the screen to mark their on a magnetic ballot card (which the voter then inserted into an electronic ballot box that automatically recorded the vote); and a full-face direct recording e-voting machine (DRE) with a button for each candidate.

Following this positive trial, the system based on the magnetic ballot card was chosen and in 1994 approximately 1.4 million voters (around 20% of the electorate) across the three regions of the country cast their votes via an automated system described in the Belgian Law of 11 April 1994 on the organisation of automated voting. The hardware and electoral software was provided by Steria (BULL) and STESUD (PHILIPS).

In 1998, further municipalities opted to use the e-voting system on a voluntary basis. It followed that more than 3.2 million voters (44% of the electorate) voted in the federal, regional and European elections in June 1999 via magnetic card voting machines.

---

[43] Some French municipalities use e-voting machines (those with over 3,500 inhabitants that had received approval from their regional department by 2008). In 2008, a moratorium on the use of e-voting machines was adopted, forbidding any expansion in the use of such equipment beyond the municipalities that were already using them.

On 14 July 2005, the first-generation equipment (from 1994) was updated so that it could be used seamlessly in the 2006 and 2007 elections. Based on the use of this automated voting system, which met expectations, a further step was taken in 2007 in the form of a study describing a new e-voting system provided with an independent voter-verifiable record (IVVR) or voter-verifiable paper audit trail (VVPAT). This system was rolled out in Belgium in 2012 and is now used in 187 municipalities (in the Flemish Region, the Brussels-Capital Region and the German-speaking Community).

Before 2012, there were two e-voting systems in use in Belgium: 'Digivote' (STERIA – 85% of the market) and 'Jites' (STESUD – 15% of the market). The source codes of the voting software were made available on an online government portal. The municipalities opting for e-voting had to choose which system they would use. Since the two systems were incompatible, all municipalities within the same electoral canton had to agree on the same system[44]. These e-voting systems were used again during elections in 2012 and 2014, but only in the Brussels and Walloon regions.

In 2018 the Walloon region ended its use of e-voting[45]. The Brussels region made the switch to the paper trail voting system already used in Flanders in 2012 and 2014. Since then, there has been a single e-voting system in Belgium, supplied by the company Smartmatic[46].

5.1.2 Legal framework

The legal framework is governed by the Law of 7 February 2014 on electronic voting (*Loi du 7 février 2014 organisant le vote électronique avec preuve papier*).

5.1.3 Brief description of the software system and technology used

Central preparation software (ECM) is developed in Java. ECM creates a 'master' USB stick for all of Belgium's electronic polling stations. This master USB stick is duplicated as many times as necessary by the central organising authority.

The voting software for the polling stations is developed in C++. Each polling station can be opened using a pair of securely distributed USB sticks generated by the central organising authority. Use of the correct login and password allows the corresponding polling station to be opened.

5.1.4 Testing methodology

There are different testing methods in use:

1. Mass testing;
2. End-to-end testing;
3. Security testing.

The supplier who develops the software will test the system to make sure that the delivery corresponds to the requirements. For each delivery, the supplier conducts all necessary testing. This includes operational tests, mass tests and usability tests.

Delivery takes place well in advance of the actual elections, so that the administration can begin its own tests. The administration receives a version of the software that is approved by

---

[44] https://www.osce.org/files/f/documents/3/9/22450.pdf

[45] Although electronic voting was used in the Walloon region from 1994 to 2014, the Walloon government decided to no longer allow its use in Walloon municipalities on account of the system's lack of transparency and high cost of use.

[46] The Smartmatic system had already been used in two municipalities (out of 19) in 2012 and 2014. For the 2018 elections, the Brussels government decided on a complete roll-out.

the companyto review. Often, the administration will receive an intermediate version for review and follow-up. During the development process, there is active follow-up by the administration and regular status meetings are held. The firm responsible is also asked to perform an annual security analysis of the system's supporting OS.

The administration conducts an end-to-end test to ensure the system provides the correct functionality and to confirm delivery. In addition, further security tests are carried out by the administration itself, along with a third party different to the software developer.

Following these tests, but before using the system in real elections, the system must also be audited by an independent control body. Only if the audit report delivers a positive opinion will the system be used in real elections. After each election, changes are made at the security and operational level in the light of technological developments and lessons learned.

The system hardware was acquired in 2012 and 2018 and is (mostly) stored in the municipalities under local supervision. To ensure that the e-voting machines work properly, the municipalities are required to test their equipment. If any hardware components are defective, the supplier will repair the machines. In non-election years 10 % of the equipment should be tested. During an election year the municipalities must test 100 % of the equipment in preparation for the elections. This is a diagnostic test that confirms the correct functioning of all the system's various hardware components (card reader, touch screen, etc.). The supplier delivers the necessary testing equipment (USB stick) to each municipality for these tests to be carried out. The results of the tests are transmitted to the supplier for analysis and any necessary repairs.

These software and hardware tests ensure the correct functioning of the system during the election period. As all these tests are conducted on a regular basis, e-voting can be used even if there are unscheduled early elections with only 40 days between the announcement of the elections and the actual polling day.

5.1.5   Functional and operational flow

Each voting booth at an electronic polling station is equipped with an e-voting machine with touch screen. Voters receive an activated smart card from the polling station's presiding officer. To cast their vote, voters first insert the smart card into the voting machine's card reader. The voting machine will then display the serial number and acronym of all the lists of candidates on the touch screen. The voter chooses a list using their finger, or they can also cast a blank vote. They can then confirm their choice or cancel it in order to choose a different list.

After voters have chosen a list, the voting machine displays the names and first names of the candidates on that list. Voters then cast their vote by tapping the screen.

Voters are then asked to confirm (approve) the vote being cast. Until their vote is confirmed, voters can still modify it (by cancelling the vote being cast) and choose another list of candidates.

As final confirmation, a ballot paper is printed by the voting machine, allowing voters to check their choices. The printed ballot acts as a Voter Verified Paper Audit Trail by replicating the choice of the voter in plain text. It also features a barcode.

Before leaving the voting booth voters fold their ballot paper in two (printed side inwards).

Voters then collect their voting smart card, scan the barcode of their ballot paper using the ballot box reader (**electronic ballot box**) and deposit their folded ballot paper in the ballot box, under the supervision of the presiding officer (or their appointed assessor). After reading the ballot's barcode, this device transfers the data to two separate USB sticks before capturing and

storing the paper ballot. Each vote is encrypted on the USB sticks. As the ballot box is equipped with a shutter that opens automatically, it is only possible to insert the ballot paper once it has been correctly scanned.
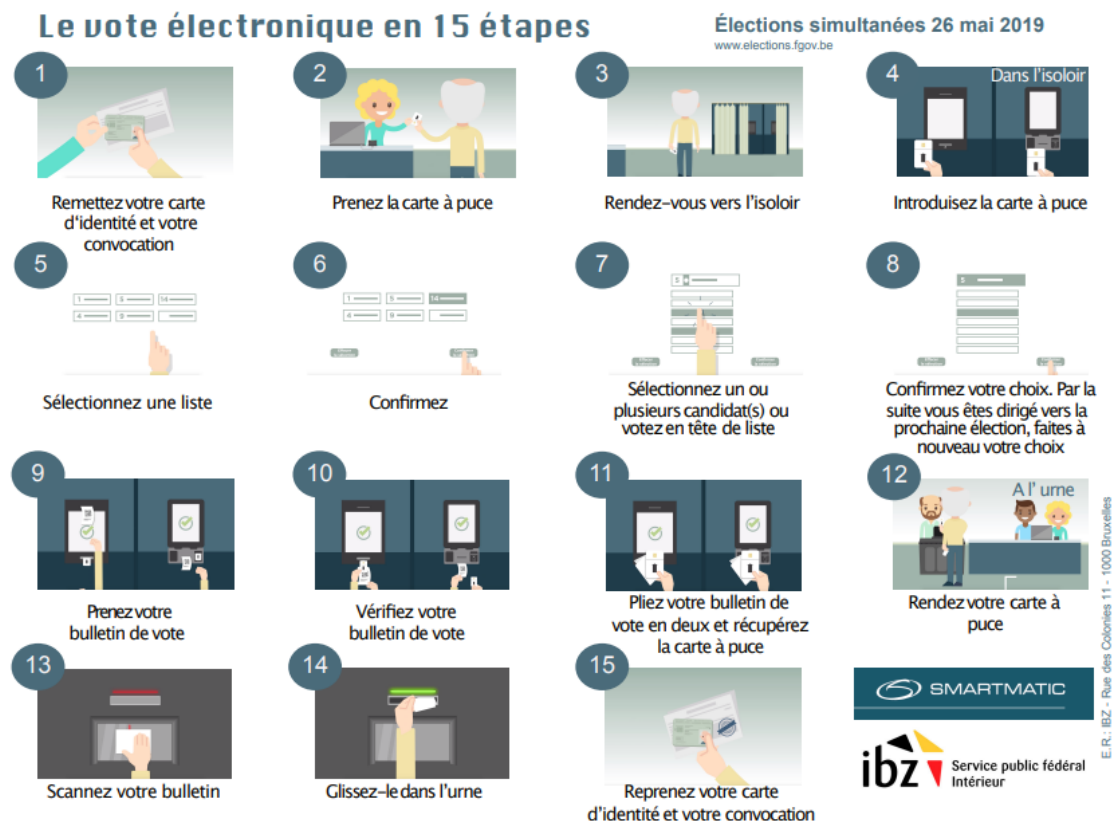
Source: https://elections.fgov.be/sites/default/files/inline-files/Le_vote_electronique_en_15_etapes.pdf

The smart card does not contain data about the vote cast. It is an activation token for initiating the voting process in the voting booth. The smart card is activated on the presiding officer's machine. Depending on how the card is activated, voters can vote in one or more elections. The smart card will be returned to the presiding officer after the voting process and reactivated for the next voter.

The presiding officer uses a separate machine to activate smart cards used by voters to access the voting machines, electronically register and store each vote, count all votes and store the results, and generate a polling station report. A polling station report does not contain any data about the actual results, but simply technical data about the result file such as a hash code and a checksum to guarantee the integrity of the results. These machines work together with peripheral devices that allow them to transfer information from the electronic ballot box.

At the end of the voting process, the presiding officer closes the polling station and sends the USB drives on which the votes are encrypted and recorded to the electoral canton's main polling centre, which decrypts and collects all data and totalises the votes.

5.1.6 Communication campaign/awareness raising, including the building of voter trust and confidence

The Elections directorate of the Federal Public Service Interior has issued guidance, including a practical manual for voters that provides an overview of the Belgian voting system in the

country's three official languages (French, Dutch, German) with video and written explanations of how to use the voting machines[47]. Aspiring voters can also use an e-voting simulation with the final lists of candidates to familiarise themselves with the various screens. There are different simulation versions in each constituency.

5.1.7 Accessibility for people with disabilities and older people

Specific attention was paid to usability aspects (learnability, efficiency, memorability, errors, and subjective satisfaction) and the needs of people with disabilities. Tests were conducted in various retirement homes, such as the usability tests carried out in 2011. Retirement home residents were asked to use the new voting system. Lessons learned were implemented before the system was first used during the 2012 elections to ensure that older people were also able to use the voting system.

New voting machines feature user-friendly interfaces, and in some cases are complemented by assistive technology to help voters with visual disabilities navigate the ballot and vote independently.

Further advances could enhance accessibility features, such as screen height, a screen reader function for blind people (including the possibility to plug in headphones to ensure the secrecy of the vote), or the possibility to magnify text.

5.1.8 Data protection and Council of Europe standards

To guarantee data protection and the secrecy of the vote, no voter data are stored in the system. Voters receive a smart card to activate the voting process, but this token does not contain any data about either the voter or the actual vote cast.

5.1.9 Threats and vulnerabilities identified and mitigation measures

The Elections directorate of the Federal Public Service Interior conducted a risk analysis with different measures to avoid or mitigate problems.

An important measure to guarantee the correct functioning of the system is an audit report conducted by an independent control body. Only if the audit confirms the correct functioning of the software can the system be used on polling day. An independent control body is selected from a list established by the organising authority. The organising authority compiles a list of requirements which audit companies can apply. The supplier is obligated to pick one of the companies on the list to carry out an audit of the e-voting system.

For hardware problems on polling day there is a technical helpdesk to resolve operational issues. A team of technicians with back-up components is on stand-by to intervene if necessary.

During the election period, a College of Experts[48] permanently supervises all technical, procedural and operational actions and prepares a report for parliament.

---

[47] https://elections.fgov.be/electeurs-comment-voter/le-vote-electronique
[48] The Federal College of Experts is a permanent independent public body whose members are appointed before the elections by the Chamber and the parliaments of the Communities and Regions. The College of Experts starts operating 40 days before election day and assesses the use and functioning of all automated voting, counting, tabulation and transmission systems, mostly through analysis of the source codes and the hardware before election day and through spot checks on election day. The experts have access to all voting machines, systems and relevant information, can visit polling stations to carry out audits at any time, and are authorised to conduct recounts of individual polling stations. The College has to deliver a report with recommendations to parliament at

5.1.10 Links to further information

Service public fédéral Intérieur, Direction des Élections, e-voting: https://elections.fgov.be/electeurs-comment-voter/le-vote-electronique

Étude sur la possibilité d'introduire le vote Internet en Belgique (4 December 2020): https://elections.fgov.be/sites/default/files/inline-files/Rapport_volet_1_4Dec2020_Def_F.pdf

Belgium, Federal Elections, 26 May 2019: Needs Assessment Mission Report, Organization for Security and Co-operation in Europe, 5 April 2019: https://www.osce.org/files/f/documents/7/f/416432.pdf

https://elections.fgov.be/

5.1.11 Contact

Directorate for Elections of the Federal Public Service Interior

elections@rrn.fgov.be

5.2 E-voting machines in the district of Évora, Portugal

5.2.1 Short description

E-voting was implemented in the district of Évora, Portugal, for the 2019 European Parliament elections. It involved the installation of 47 electronic polling stations (94 digital ballot boxes) in 25 parishes of the district's 14 municipalities. The e-voting polling stations were independent and additional to the conventional polling stations, allowing voters to choose either the traditional voting method or the electronic vote.

5.2.2 Legal framework

The legal basis for e-voting is Organic Law No 3/2018, of 17 August, which states that the General Secretariat of the Ministry for Home Affairs – Electoral Administration *'in the next electoral act for the European Parliament […] may promote the implementation, as an experiment, of the electronic vote in person, in at least 10 national municipalities, being the votes cast during the tabulation of the results'.*

Law No 70/2018 of 31 December laid the groundwork for the implementation of a pilot-project on in-person e-voting as well as on the dematerialisation of the electoral rolls. Under Portuguese electoral law, the electronic vote was designed in accordance with the following principles:

- Universality: the system covered all eligible voters in the district of Évora.

- Confidentiality of the vote: guaranteeing the absolute confidentiality of how people voted.

- Unicity: ensuring respect for the principle of 'one voter, one vote'.

- Reliability: the system must produce accurate results.

---

all levels and to the Federal Public Service Interior within 15 days after the elections – https://www.osce.org/files/f/documents/7/f/416432.pdf

- Personal and on-site vote: Article 49(2) of the Portuguese Constitution must be upheld, according to which 'The exercise of the right to vote is personal and constitutes a civic duty'. Article 121(3), which establishes that 'the right to vote on national territory is exercised in person', must also be upheld.

5.2.3 Brief description of the software system and technology used

The CED (dematerialised electoral rolls) system allowed computer access to information in a centralised database. Both the database and the server software components were housed in the infrastructure of the National Internal Security Network (RNSI), which was already used for other electoral support systems. The system thus benefitted from the central infrastructure, as well as all operation, maintenance, and security services available, since all components of the CED system (both the infrastructure and the software itself) are always protected by several layers of security.

For software components, the CED used a web application with service-oriented architecture (SOA) and a Representational State Transfer (REST) service architecture.

A Single Page Application (SPA) approach was used in the visual component of the CED, in which the visual component of the web application was downloaded only once when first accessed, with subsequent access involving no more than the exchange of data with the web service. This approach is designed to ensure maximised performance and use of the application in environments with reduced bandwidth, given the limitations identified in some polling stations due to poor indoor 3G/4G network coverage, and the construction typology of some of the buildings used as polling stations.

Access to the CED was controlled through authentication with username and password, and the credentials of the polling officials were provided in physical format on election day. All REST service operations required authentication, using a token generated at the point of authentication and used transparently in subsequent user requests.

The REST service provided authenticated users with access to controlled functionalities for managing the polling station and its registered voters, according to the defined system requirements. This service allowed information to be stored in a centralised transactional database, which meant that activities could be synchronised and coordinated between all polling stations.

All CED software components were installed and made available in the infrastructure managed by RNSI, except for a component that granted access to the Portuguese 'citizen card' and which was installed locally in each of the computers. This component allowed the CED system to obtain public data on all citizen cards, in particular the bearer's photograph and identification number.

The second-generation systems record the vote in two independent formats: digital and physical (paper). The latter can be audited by means which are independent from the voting equipment software. These paper-based e-voting solutions are known as IVVR or VVPAT.

The system used in e-voting consisted of computerised equipment for the direct scrutiny of votes through selection on a touch screen. The equipment was activated using a voting login token provided to the system through a smart card (SC).

The system was rounded off by the Election Management System (EMS) electoral process configuration platform, which allowed the electoral management body (EMB) to create and configure all the e-voting systems to be installed in the e-voting sections, the respective databases, the smart cards of polling station staff and the encryption keys used to protect and identify these systems.

The overall components of the various tools that made up the e-voting system consisted of: P&V ECO, touch screen, printer, UPS (uninterruptible power supply), VIA smart cards (voting cards), headsets, electronic voting booth, audio lock and compact flash (CF) memory card.

5.2.4 Testing methodology

Three trials and simulations took place over a three-week period on 11, 18 and 25 May 2019, as follows:
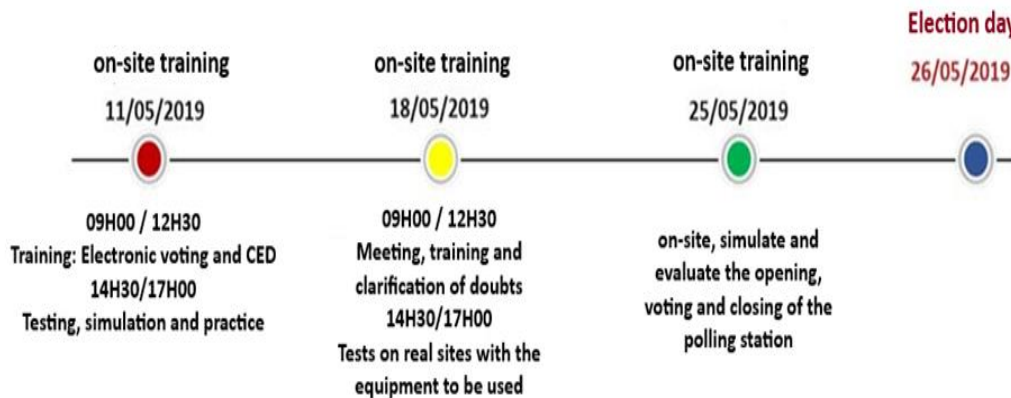
The training programme consisted of practical and theoretical components, thus allowing all staff to learn the various parameters necessary for the comprehensive handling of the equipment on election day. Tests and simulations were carried out to ensure that all polling staff rehearsed and tested all the procedures which they would be performing on election day.

The testing session was open to the public and members of the public were invited to test the e-voting equipment and simulate its use.

5.2.5 Functional and operational flow

At electronic polling stations in the district of Évora, voting took place as follows.

Initial preliminary operations included:

1) Execution of the preliminary opening operation.
2) Opening of the envelope containing the equipment's access credentials.
3) The presiding officer or, in their absence, the deputy presiding officer, opened the voting section installed in the voting booth by inserting the presiding officer's or the deputy's card, selecting the option 'Opening of the section' and printing the machine's initial report (to ensure that the machine had not registered any votes at that stage).
4) Polling station staff activated the session in the CED.
5) The polling station's presiding officer activated it in the CED application.

Voting then took place as follows:

1) The voter entered the polling station and identified themselves.
2) The voter exercised their right to vote.
3) Once the voter was recognised in the CED, a voting card was issued to them to allow them to exercise their right to vote once.
4) After casting their vote in the electronic booth and confirmation of the voter's voting intention, the vote cast was registered in the machine, at which point it could no longer be modified. The supporting document was then printed, which was folded in four, as

displayed in the instructions, and the voter delivered both the supporting document and the voting card to the polling station's presiding officer. After this step, the two tellers discharged the voter in the CED application.

Finally, the presiding officer at the polling station closed the voting process in the CED, and all polling station staff logged off the session in the application. While closing down the electoral operations, a report on the results was printed.

Figure 1 E-voting steps
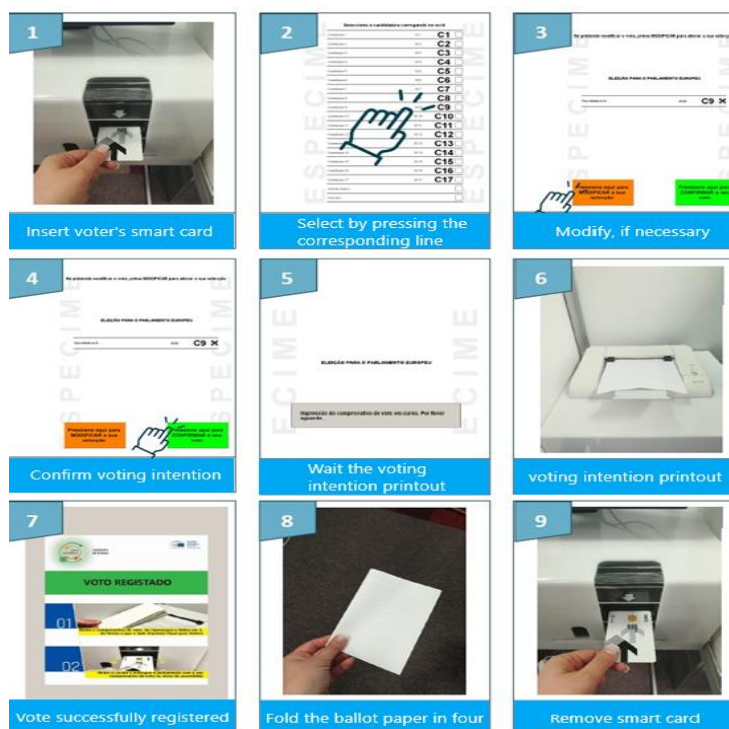
Source: Electoral Administration Unit – Portugal

5.2.6 Communication campaign/awareness raising, including building voter trust and confidence

To increase security and trust in the electoral process, communication and information campaigns were devised and distributed through various platforms (press, radio, television, digital media). In addition, both security audits and process audits were conducted to build voter trust and confidence.

The communication plan was based on two pillars: (1) internal communication directed at all the organisations involved in the electoral project; and (2) public communication throughout the electoral cycle. These activities contributed to greater electoral transparency and were decisive in building confidence in the e-voting system.

While low trust and acceptance are an inherent risk in such modernisation efforts, the experience in Évora shows firm acceptance among voters and politicians[49].

The decision to print a 'paper ballot' when the vote is cast in the e-voting equipment was a fundamental requirement of the e-voting system's design. By adopting the VVPAT model, a paper ballot receipt was issued (similar in all respects to a traditional ballot paper), which was placed in a ballot box and retained for possible post-election system audits. The second-generation systems record the vote in two independent formats: digital and physical (paper). The latter can be audited by means independent of the voting equipment software. This also allowed each voter to validate their votes, thus increasing confidence in the system for three reasons: first, the voter could check that their vote on the screen corresponded to the 'paper ballot'; second, in the event of a complaint it would be possible to compare the number and intentions recorded on the 'paper ballots' stored in the ballot box and the electronic votes recorded in the electronic voting equipment; third, the voting process remained simple.

5.2.7 Accessibility for people with disabilities and older people

Electronically assisted voting was available for people with visual impairments. This allowed them to interact with the e-voting system, choosing the option 'No' (by tapping the left side of the screen) or the option 'Yes' (by tapping the right side of the screen), as shown in the figure below. These instructions were transmitted to voters with visual impairments through earphones provided by the polling station. Electronic voting booths complied with accessibility requirements and ensured voter confidentiality.

---

[49]

https://www.sg.mai.gov.pt/AdministracaoEleitoral/EleicoesReferendos/ParlamentoEuropeu/Documents/Final%20Report%20%E2%80%93%20Electronic%20voting%20%E2%80%93%20European%20Parliament%20Elections%20(VF).pdf

Figure 2 Steps to exercise assisted e-voting

Source: Electoral Administration Unit – Portugal

Conventional voting, as laid down in the legal norms applicable to elections, was respected, with the necessary adaptations, by polling station staff in the district of Évora who carried out voting and partial counting operations.

5.2.8   Data protection and Council of Europe standards

In the polling stations set up in the district of Évora, access to the CED made it possible to:

- verify, by inserting the citizen card or searching by name or identification number for the voter's entry in the electoral register. E-voting stations had full access to the electoral roll for the district of Évora. Conventional polling stations only had access to the electoral roll corresponding to the respective polling station;

- validate that the voter who wished to exercise their right to vote at a conventional polling station had not yet cast a vote in any other polling station in the district of Évora. Alternatively, in the case of an electronic polling station, whether the voter had not yet done so in a conventional polling station where they were registered, or in any other electronic polling station in the district;

- Record the exercising of the right to vote in the dematerialised electoral roll by electors who voted at that polling station.

The CED information system contained simplified information on registered voters, but its database was not downloaded locally to the computers installed in the conventional or electronic polling stations. Instead, access was provided through a set of individual credentials (user and password) which were distributed in person on election day in a closed and sealed envelope. Access to personal data in the CED could be provided by the system administrators, for maintenance and administration operations, and by polling station staff, who by law already had access to this data in the exercise of their functions (through the electoral roll in paper format).

The laptops installed at the polling stations in the district of Évora were managed by RNSI itself and had no access to the internet or to any internal network, only to the CED information system through its own circuits. Since personal data were contained in the encrypted CED database, all operations undertaken in the system were traceable. After all polling stations had been closed and voter reports submitted for intermediate tabulation, the table containing sensitive voter data was deleted from the CED information system. The remaining information was deleted after publication of the official election results by the National Election Commission (CNE) in the Official Gazette. The CED system did not access or interconnect with any other information systems and databases.

Pursuant to the GDPR, the data protection officer of the General Secretariat of the Portuguese Ministry for Home Affairs was involved, as and when required, in matters related to the protection of personal data and the respective processing operations. In compliance with the GDPR, voters were informed about the processing of data necessary for the availability of the CED on posters positioned near each polling station in the district. These posters indicated that: (1) the General Secretariat of the Ministry for Home Affairs was the body responsible for data processing; (2) the sole purpose of processing was to ensure the exercising of the right to vote of electors registered in the district of Évora and to guarantee the unicity of the vote; (3) the data collected would be destroyed at the end of voting and local tabulation operations, after sending a report to the Intermediate Tabulation Assembly; and (4) that the data available in the dematerialised electoral registers was intended solely and exclusively for voting and tabulation operations, with no further processing carried out.

Regarding the analysis of compliance with the Council of Europe recommendations in the implementation of e-voting in the district of Évora, it is important to underline the following:

- E-voting was implemented gradually and progressively;

- The public, in particular voters, had been informed well in advance of the start of voting, in clear and simple language, about the e-voting timetable, the correct use and functioning of the e-voting system, and the necessary steps to participate and vote;

- The e-voting system was auditable, open and comprehensive, and potential issues and threats were actively reported;

- The voter interface of the e-voting system was easy to understand and use;

- The e-voting system was designed, as far as it is practicable, to enable people with disabilities and special needs to vote independently;

- All official voting information was presented in an equal manner, within and across voting channels;

- The e-voting system ensured that only the appropriate number of votes per elector was cast, stored in the electronic ballot box, and included in the election result;

- Voting intentions were not affected by the voting system, or by any undue influence;

- The way in which voters were guided through the e-voting process did not lead them to vote with undue haste or without confirmation of their vote;

- Voters were able to verify that their voting intention was accurately represented in the vote and that the sealed vote was recorded in the electronic ballot box without alteration;

- E-voting was organised to ensure respect for the secrecy of the vote at all stages of the voting procedure;

- The e-voting system and all authorised parties protected authentication data so that unauthorised parties could not misuse, intercept, modify or otherwise gain knowledge of these data;

- The e-voting process, in particular the counting stage, was organised in such a way that it was not possible to reconstruct a link between the unsealed vote and the voter;

- Only persons authorised by the EMB had access to the central infrastructure, servers and election data.

5.2.9 Threats and vulnerabilities identified and mitigation measures

After the CED system's first use in a real election, it was possible to identify situations in which this system worked correctly and provided benefits, as well as others in which improvements could be implemented for any future use of the system.

Polling station staff are the main parties responsible for the electoral procedures and it is therefore vital that they learn the necessary operations for e-voting. Once this risk was identified, polling station staff received adequate training to ensure they were able to perform all the necessary operations without difficulty. During the project's development, special attention was paid to simplifying the voting procedure and the remaining procedures on election day, both of which are the responsibility of polling station staff (opening, closure, printing of results).

To counter the risk of possible failure in the tabulation and transmission of final data in the framework of provisional scrutiny as well as to ensure consistent data provision by all entities involved, access to the CED through the contact centre was provided as a contingency measure to complement the local infrastructure in each of the polling stations.

This channel was designed to be used exclusively by polling station staff if ever the system became inaccessible from polling stations, possibly as a result of temporary failures of computer or communications equipment, network connection failures to the RNSI or power supply outages. It could be accessed by a polling station staff member using the credentials assigned to them on election day, after automatic validation by an Interactive Voice Response (IVR) system, in exchange for providing a password and counter password through a call made to their mobile phone, and subsequent identification of the polling station staff member by the contact centre operator. After automatic validation, the polling station staff member would be connected to a telephone operator, who could interact with the CED system on behalf of the polling station staff member contacting them. The contact centre operator did not have any individual capacity to access the CED, but instead required a contact and positive identification from a polling station staff member to perform the actions mentioned over the phone on their behalf. All operations performed by the operator on behalf of the polling station staff member had to be logged in the CED application and the telephone call was also recorded.

Another vulnerability identified in advance included possible security failures and intrusion by third parties in the database systems, but no issues were encountered. Since the e-voting equipment operated offline and there was no transmission or integration with any communication network, the risk of cyber interference was eliminated.

5.2.10 Links to further information

All available information relating to the 2019 European Parliament elections and the e-voting solution implemented is available at:

https://www.sg.mai.gov.pt/AdministracaoEleitoral/EleicoesReferendos/ParlamentoEuropeu/Paginas/default.aspx?FirstOpen=1

The English version of the final report on the implementation of e-voting in the district of Évora during the 2019 European Parliament elections is available at:

https://www.sg.mai.gov.pt/AdministracaoEleitoral/EleicoesReferendos/ParlamentoEuropeu/Documents/Final%20Report%20%E2%80%93%20Electronic%20voting%20%E2%80%93%20European%20Parliament%20Elections%20(VF).pdf

5.2.11 Contact

General Secretariat of the Ministry for Home Affairs – Electoral Administration Unit: adm.eleitoral@sg.mai.gov.pt; +351213947100

5.3 France's internet voting system for French citizens resident abroad

5.3.1   Short description

France offers remote e-voting for two types of elections: legislative and consular elections. However, remote e-voting in these two types of elections is only available to French citizens resident abroad who are registered on a consular list and who have provided a valid email address and a mobile phone number[50]. The e-voting method is an internet voting system accessible via a computer, tablet, or mobile phone with an internet connection.

---

[50] *France Diplomatie, Vote par internet:* https://www.diplomatie.gouv.fr/fr/services-aux-francais/voter-a-l-etranger/modalites-de-vote/vote-par-internet/

This solution was first implemented in 2012, and it was most recently made available for legislative elections in June 2022. Participation in the elections using this system increased sharply after 2014, as shown in the figure below. During the first and second rounds of the 2022 legislative elections, e-voting was available for 5 consecutive days, from the Friday before the first round until the Wednesday before the second round.

Figure 3 Share of registered voters who used internet voting in each election.
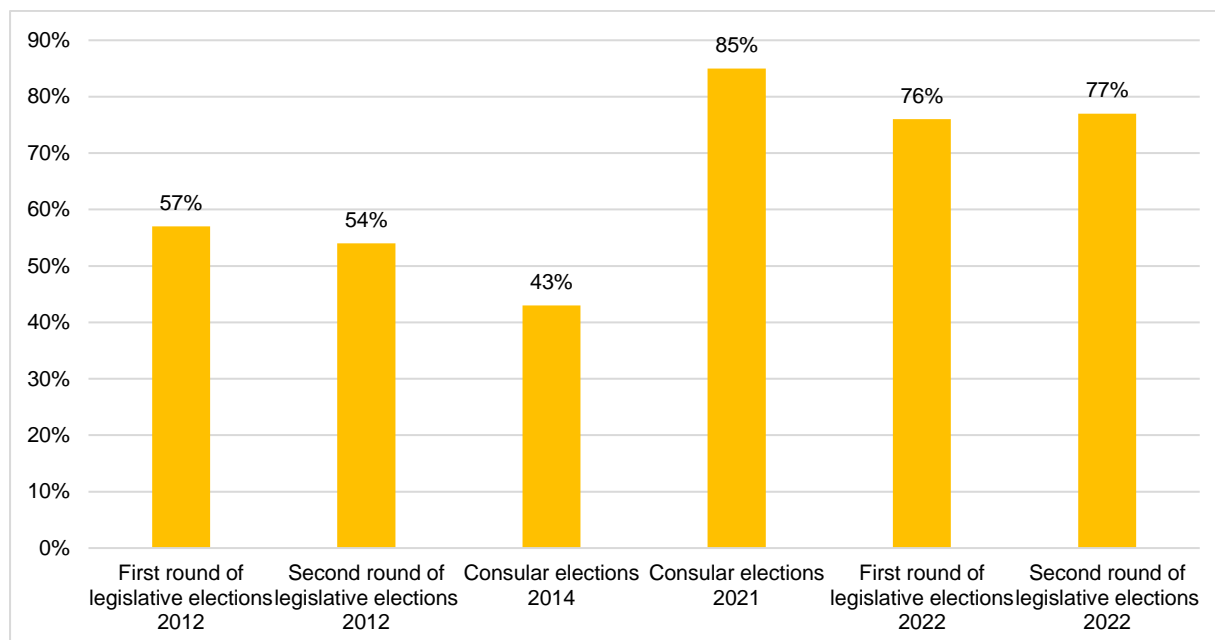
Source: *Secrétariat général des affaires européennes, Pratique du vote par internet en France: une modalité de vote à disposition des Français de l'étranger lors des élections consulaires et législatives.*

5.3.2   Legal framework

Article 3 of the French Constitution stipulates that all French citizens of whatever gender who have reached adulthood and are in possession of their civil and political rights may vote. According to Article R176-3 of the French Electoral Code[51], French citizens resident abroad can vote remotely using electronic means. The procedural framework takes data protection rules into account, and voters are explicitly granted data protection rights[52]. An 'Office of Electoral Votes' was established to supervise the correct functioning of the e-voting system[53]. The identity of the voter is verified with a password that is not connected to their civil status[54]. After the voter is identified by the system, the citizen can cast their vote. Once the system has registered the vote it will send a confirmation code to the citizen[55].

5.3.3   Brief description of the software system and technology used

France has changed the supplier of its e-voting system several times since it introduced e-voting. From 2012 to 2014, the consortium formed by ATOS/Scytl was responsible for the delivery of the service, with Scytl providing the voting software and ATOS hosting the voting platform. In 2016, Scytl won the tender to provide the voting software as well as a tool to manage the results of the 2021 consular elections. The servers for both the voting software

---

[51] https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070239/LEGISCTA000024372035/
[52] Article R176-3 of the French Electoral Code.
[53] Article R176-3-1 of the French Electoral Code.
[54] Article R176-3-7 of the French Electoral Code.
[55] Article R176-3-9 of the French Electoral Code.

and the tool to manage the results were based in France and hosted by NTT. Finally, in 2019, the French government published a new tender to find a provider for the 2022 legislative elections. The winner was the French company Voxaly-Docaposte. During these 2022 elections, the Voxaly-Docaposte system was hosted by the Ministry for Europe and Foreign Affairs (MEAE in French)[56]. In France, it is not compulsory for providers of software tools to the public sector to publicly disclose the characteristics of the system used[57].

5.3.4   Testing methodology

The testing stage of the e-voting mechanism for the legislative and consular elections in France was crucial, given that in 2017 the system was not used due to cybersecurity concerns[58]. The French government conducted two full-scale tests of the e-voting system reproducing real-life conditions. In these full-scale tests, volunteers were recruited from around the world, representing around 1 % of the electorate. During the tests, the voting platform was open twice, for 72 hours each time (imitating the two-round system of voting used in France), and voters were asked to follow the same voting procedure as they would in a real election. The first test took place in September 2021 and the second in January 2022. The supplier of the e-voting system used the four-month gap to improve the voting procedure. The tests were audited by an independent expert, with advice from experts of the French cybersecurity agency (ANSSI), and supervised by the e-voting committee[59]. At the end of the tests, the president of the e-voting committee (who is a member of the State Council) reported that the tests were conclusive, and that the results ensured that e-voting would comply with the requirements for holding a secure and trustworthy election[60].

5.3.5   Functional and operational flow

The voting process consisted of several steps. Four days before the opening of the e-voting platform, registered voters received two codes: one via email with a username, and another via an SMS containing a password. The e-voting platform was then open for 5 days during each election round. During this period, the voters had to follow the steps set out in the bullet points below.

- First, they had to access the website of the French diplomatic service and click on the 'I vote via the internet' option.
- They were then prompted to identify themselves using the username and password they had previously received via email and SMS.
- Once the identification process had been successfully completed, they were redirected to a page where they had to either select the candidate they wanted to vote for or cast a blank vote. In accordance with French electoral law, the candidates appeared in the order fixed randomly at the moment the candidate registration period is closed.
- After clicking on 'Next', voters were asked to confirm their choice on a new screen.
- When they clicked 'Confirm', they were redirected to the voting page. To validate their vote, they had to enter a code sent by email within 10 minutes after confirmation. The code they received was valid for 15 minutes.

---

[56] *Secrétariat général des affaires européennes, Pratique du vote par internet en France: une modalité de vote à disposition des Français de l'étranger lors des élections consulaires et législatives.*

[57]   https://www.francetvinfo.fr/elections/legislatives/legislatives-comment-fonctionne-le-vote-par-internet-accessible-aux-francais-de-l-etranger_5161495.html

[58] https://monaco-hebdo.com/dossier/vote-electronique-legislatives-2022/

[59] https://www.diplomatie.gouv.fr/fr/services-aux-francais/voter-a-l-etranger/modalites-de-vote/vote-par-internet/#sommaire_5

[60] https://monaco-hebdo.com/dossier/vote-electronique-legislatives-2022/

- After entering the code, the 'Vote' button became visible on the voter's screen, and voters had to click on this 'Vote' button to officially cast their vote.
- Finally, a new screen appeared with the message that the vote had been correctly cast. Simultaneously, voters received the same confirmation by email. On this final screen, voters were asked to download the voting receipt, with the warning that it would not be available once they left the page.

Figure 4 E-voting process

| Reception of credentials | Access voting platform | Voter identification | Selection of candidate | Confirmation of selection | Input voting code | Vote | Download voting receipt |

Source: *https://alliancesolidaire.org/2022/05/25/vote-electronique-pour-les-elections-legislatives-des-francais-de-letranger-suivez-le-guide/*

After an individual has voted, their vote is encrypted and sent to the server. Once counting is automatically completed, the system delivers the result and cryptographic proof that the results correspond to the sum of encrypted votes. In the most recent election, a group of experts from the National Centre of Scientific Research (CNRS) was tasked with verifying that there were no issues with the cryptographic proof[61].

5.3.6 Communication campaign/awareness raising, including building voter trust and confidence

The website of the French diplomatic service provides information on the steps required to vote using the e-voting system, the correct use and functioning of the e-voting system, and all stages of the e-voting timetable[62]. To increase trust in the system, the page also provides detailed information about both the approval process for the e-voting system, and the tests conducted to ensure its proper functioning[63]. In addition, consular webpages also provided information about e-voting for French citizens resident abroad.

5.3.7 Accessibility for people with disabilities and older people

Accessibility to internet voting is provided for under of 11 February 2005 on the equal rights and opportunities, participation and citizenship of people with disabilities. Its implementing decree No 2019-768 of 24 July 2019 relates to the accessibility of online public communication services for people with disabilities.

When a website, in this case the Internet voting site, is simultaneously subject to the accessibility obligations imposed by this legislative provision, and those prescribed by the legal and regulatory provisions relating to the fight against discrimination and transposing Directive 2000/78/EC, the assessment of the scope and level of accessibility obligations is based on the most favorable provisions for accessibility in each of these two categories of rules.

The inter-ministerial digital directorate (DINUM) publishes the general repository for improving accessibility (RGAA Version 4.1) to facilitate access for people with disabilities to the webpages of digital solutions. The interaction between people with disabilities and webpages must comply with the control criteria of the RGAA. These criteria contain mandatory technical tests relating to the structuring and presentation of information, particularly for forms, navigation

---

[61] https://www.francetvinfo.fr/elections/legislatives/legislatives-comment-fonctionne-le-vote-par-internet-accessible-aux-francais-de-l-etranger_5161495.html
[62] https://www.diplomatie.gouv.fr/fr/services-aux-francais/voter-a-l-etranger/modalites-de-vote/vote-par-internet
[63] https://www.diplomatie.gouv.fr/fr/services-aux-francais/voter-a-l-etranger/modalites-de-vote/vote-par-internet/

and consultation, and non-mandatory tests relating to images, frames, colours, links, scripts and multimedia.

The General Repository for Improving Accessibility (RGAA Version 4.1) is a tool for evaluating and improving access by people with disabilities to the webpages of digital solutions. According to the audit of RGAA Version 4.1 carried out before the June 2022 legislative elections, the VPI solution offered by the Ministry for Europe and Foreign Affairs to French people resident abroad was 78 % compliant with this reference.

In 2019, the French Senate[64] discussed the merits of e-voting in improving accessibility for people with disabilities, specifically people with reduced mobility and people with visual impairments, compared to conventional, in-person, paper-based voting. According to the French Ministry of the Interior, conventional polling stations and existing e-voting machine models already guarantee a high level of accessibility, regardless of age and disability. In this regard, the physical infrastructure at polling stations is organised to ensure accessibility for all. Furthermore, voting officials must guarantee that at least one voting booth is adapted to the needs of voters with disabilities. Additionally, disabled people in need of physical assistance can request the presence of another elector to assist them in the voting booth.

5.3.8 Data protection and Council of Europe standards

Voxaly-Docaposte reports that it complies with the National Commission of Information and Freedoms[65] (*Commission Nationale de l'Informatique et des Libertés* – CNIL) 2019 recommendation[66], which is specific to France and focuses on the security of voting systems. This recommendation is currently the most comprehensive set of advice specifically addressing online voting systems in France.

The CNIL 2019 recommendation refers to Convention 108 of the Council of Europe on the protection of individuals regarding the processing of personal data, as well as the GDPR.

CNIL Security Objectives[67]		Does Voxaly's system comply?[68]
Security Objectives – Level 1	1. Implement a high-quality technical and organisational solution that does not present any major flaws	YES
	2. Define the vote of an elector as an atomic operation comprising choice, validation, registration of the vote in the ballot box, signature and delivery of a receipt.	YES
	3. Authenticate voters by ensuring that major risks related to identity theft are significantly reduced.	YES

---

[64] https://www.senat.fr/questions/base/2019/qSEQ190610758.html

[65] The *Commission Nationale de l'Informatique et des Libertés* (CNIL) is an independent administrative body founded in 1978, responsible for ensuring data protection regulations and digitalisation for the public good in France (https://www.cnil.fr/fr/cnil-direct/question/la-cnil-cest-quoi).

[66] Full title: *Délibération n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet.*

[67] *Délibération n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondence electronique, notamment via Internet.*

[68] https://www.voxaly.com/blog/vote/eclairages-sur-la-nouvelle-recommandation-cnil-2019-applicable-en-2020/

	4.	Ensure the strict confidentiality of the ballot from its creation on the voter's computer.	YES
	5.	Ensure the strict confidentiality and integrity of the ballot during transit.	YES
	6.	Ensure the strict organisational and/or technical confidentiality and integrity of the ballot during processing and while stored in the ballot box until counting.	YES
	7.	Ensure full separation between the identity of the voter and the expression of their vote for the entire duration of processing.	YES
	8.	Reinforce the confidentiality and integrity of data by distributing secrecy to allow counting exclusively within the electoral office and guarantee the possibility of counting from a predetermined secrecy threshold.	YES
	9.	Define counting as an atomic function usable only after voting has closed.	YES
			YES
	10.	Ensure the integrity of the system, the ballot box and the attendance list.	YES
	11.	Ensure that counting of the ballot box can be verified a posteriori.	YES
Security Objectives – Level 2	1.	Ensure the system's high availability.	YES
	2.	Ensure automatic control 'of the integrity of the system, ballot box and attendance list.	YES
	3.	Allow automatic control by the electoral office of the integrity of the voting platform throughout the ballot.	YES
	4.	Authenticate voters by ensuring that major and minor risks associated with identity theft are significantly reduced.	YES
	5.	Ensure logical partitioning between each voting service so that it is possible to stop a vote entirely without this having the slightest impact on the other votes in progress.	YES
	6.	Use an IT system implementing the security measures recommended by publishers and ANSSI.	YES
	7.	Ensure the transparency of the ballot box for all voters.	YES
Security Objectives – Level 3	1.	Study the risks using a proven method to define the most appropriate measures in the context of implementation.	Available on request

	2. Enable ballot box transparency for all voters using third-party tools.	Available on request
	3. Ensure very high availability of the voting solution by considering the risks of major damage.	YES
	4. Allow automatic and manual control by the electoral office of the integrity of the platform throughout the ballot.	YES
	5. Ensure physical partitioning between each voting service so that it is possible to stop a vote entirely without this having the slightest impact on the other votes in progress.	Available on request

Source: 2023 Study on E-Voting practices in the EU

5.3.9 Threats and vulnerabilities identified and mitigation measures

The experience of many French citizens in the most recent election (i.e. the legislative election in 20xx) shows some of the challenges of e-voting. For instance, authorities struggle to find a balance between cybersecurity, including voter identity, and process simplification. A post-election survey conducted by the People 2022 project (led by ESPOL Lille) is noteworthy in this respect. While most respondents stated that they are in favour of and would use e-voting, 60.7 % of those who would not use e-voting cited security as the main reason for not doing so. A further 20.7 % cited their lack of previous experience with the system for not using e-voting. For those willing to use e-voting, the most cited reason was efficiency: e-voting would take less time than voting at a polling station. 45.9 % would opt for e-voting because they use the internet daily. Security concerns were mitigated by increasing transparency around the testing methods used to validate and select e-voting systems. As mentioned above, the main webpage of the French diplomatic service published information on how to vote online, including a simple but comprehensive explanation of the approval procedures and the tests conducted before implementation[69].

Experts also expressed concerns about the particularities of the processes and systems used for e-voting. One major criticism related to how voters were sent important identifying information to vote (usernames, passwords and confirmation codes) via email and SMS. It has been argued that hackers could intercept the unencrypted emails. Messages sent by SMS' could also be threatened by failures in mobile telephone networks and dependency on foreign operators. Finally, if a voter used their smartphone to receive the SMS, and the email infected their device with spyware, a hacker could access the voter's voting credentials[70]. There are alternatives to using email and SMS, which would make the identification process less prone to hacking. For instance, in Estonia, all its nationals have a state-issued digital identity card that is used for all e-Government purposes, including e-voting[71]. France is taking steps towards

---

[69] https://www.diplomatie.gouv.fr/fr/services-aux-francais/voter-a-l-etranger/modalites-de-vote/vote-par-internet
[70]

http://www.acbm.com/pirates/25897_Nous_avons_essaye_le_vote_en_ligne_a_la_francaise_nos_doutes_sur_la_securite.html
[71] https://e-estonia.com/solutions/e-identity/id-card/

enabling a digital identity for its nationals. Currently, an application to prove an individual's identity online is being tested to make online public services more easily accessible and secure[72]. If successful and approved, the new digital identity will allow citizens to, among other actions, make a request for vote delegation and register in the electoral registry. [73]

Apart from vulnerability to external threats, there are concerns about the secrecy of the vote and the authenticity of the results[74], given that the knowledge required to understand what happens between the moment a vote is cast and the moment the results are delivered is beyond most people's technical grasp. To partially address this, CNIL recommended enabling ballot box transparency for all voters so they can see that the results are authentic and correspond to the votes cast[75]. Voters receive a vote receipt showing both a link to the third-party tool's website and a reference of their ballot. After the counting is finished, voters can copy and paste their ballot reference on this website and verify that their ballot was indeed deposited in the ballot box and that their ballot was counted in the results.

5.3.10 Links to further information

Elections website: https://www.diplomatie.gouv.fr/fr/services-aux-francais/voter-a-l-etranger/modalites-de-vote/vote-par-internet

Contact

French General Secretariat for European Affairs

(*Secrétariat général des affaires européennes – SGAE*):

https://sgae.gouv.fr/sites/SGAE/accueil.html

5.4 Internet voting system in Estonia

5.4.1 Short description

Work on implementing **internet voting** in Estonia started in 2002, when new electoral legislation made internet voting possible for the first time. The aim of the law was to introduce internet voting for legally binding elections. This goal was achieved in the 2005 municipal elections, when all voters could choose to vote online – all they needed was an ID card, a card reader, and a computer. The internet voting system was procured by Estonia's National Election Committee and designed from the ground up for the Estonian elections. Notably, there was little, if any, public and political debate regarding internet voting at the time.

The main reasoning behind the introduction of internet voting was to increase voter turnout and to engage younger voters. The secondary goal was to introduce a new e-service to the already lively ecosystem of e-enabled services provided by the state. For the voters, internet voting was intuitive and easy-to-use, since similar digital authentication and signing features were in use for all state and municipal services.

---

[72] https://france-identite.gouv.fr/
[73] https://france-identite.gouv.fr/en-savoir-plus/a-quoi-sert-il/
[74] https://monaco-hebdo.com/dossier/vote-electronique-legislatives-2022/
[75] https://www.francetvinfo.fr/elections/legislatives/legislatives-comment-fonctionne-le-vote-par-internet-accessible-aux-francais-de-l-etranger_5161495.html

When thinking about introducing internet voting, it is worth considering how much supporting infrastructure already exists, e.g. whether there is a secure and usable digital authentication and signing solution, and if there is a way to create electronic voter lists. The answers to these questions also determine how reliable, easy-to-use and universal the system is going to be. In Estonia, ID cards that can be used for authentication and signing were introduced in 2000 as primary ID documents and are issued to each resident[76]. Electronic voter lists are created on the basis of data in the centralised population register.

5.4.2 Legal framework

Adopted in 2002, the Riigikogu Election Act[77] provided for the possibility of internet voting, with a clause stipulating that it would not be implemented before 2005. Since then, the law has been amended several times. The organisation of internet voting is within the remit of the State Electoral Office. The National Electoral Committee's resolutions lay down the technical requirements that ensure the general principles and organisation of electronic voting. The Identity Documents Act[78] regulates the issue of identity documents, including the identity card (ID card) and a digital identity card in mobile ID form. The Electronic Identification and Trust Services for Electronic Transactions Act regulates electronic identification and trust services for electronic transactions[79].

5.4.3 Brief description of the software system and technology used

The internet voting system in its current guise has been in use since the 2017 municipal elections. It was designed: (i) to be modular (i.e. different components can be run by different institutions); (ii) to be scalable (the software can be used for various types of elections); and (iii) to use both an Elgamal algorithm to securely encrypt votes, as well as e-ID solutions to digitally sign the encrypted vote. The system was procured following a public tender and the code belongs to the election administration, allowing the source code to be made public. The code is available at GitHub[80].

5.4.4 Testing methodology

Before each election, the risk analysis plans and risk management plans are updated, and penetration tests are performed on the system. The system is also audited before each election via an ISKE security audit[81], as well as via a separate audit of internet voting procedures commissioned by the Estonian Ministry of Economics and Communications. The ministry also issues a separate assessment of election cybersecurity before each election.

5.4.5 Functional and operational flow

In preparation for each election, several working groups are created to enable information exchanges between all the participating institutions. There are four main working groups as set out in the bullet points below.

---

[76] Estonian ID cards do not record user's personal data. Instead, the ID card can be used to access personal data in a database – i.e. the card has no information about the voter's eligibility but authentication using the ID card enables the i-voting system to identify the voter and determine whether they are eligible to vote.

[77] English text available at: https://www.riigiteataja.ee/en/eli/514122020002/consolide (01/01/2021)

[78] English text available at: https://www.riigiteataja.ee/en/eli/504072022003/consolide (02/07/2022)

[79] English text available at: https://www.riigiteataja.ee/en/eli/518102021002/consolide (25/10/2021)

[80] https://github.com/vvk-ehk/ivxv. Licensed under Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License.

[81] Three-level IT Baseline Security System ISKE; based on a German IT Baseline Protection Manual (IT-Grundschutz). Replaced by E-ITS (Estonian Information Security Standard) audit starting from 01/01/2023.

1) Internet Voting Task Force – directly responsible for resolving internet voting issues and incidents. The State Electoral Office and State Information System Authority appoint its members.
2) ICT Working Group – coordinates preparation of election information systems for elections in general (State Electoral Office, State Information System Authority, Ministry of Economics and Communications).
3) Public Relations Working Group – its tasks include voter awareness campaigns, media monitoring, and preparations for countering disinformation attacks (State Electoral Office, Government Office, State Information System Authority, Ministry of Foreign Affairs, Ministry of the Interior).
4) Voter Registration Working Group – ensures that up-to-date voter lists are created on time and that voter information sheets are sent to voters in due course (State Electoral Office, Ministry of the Interior and its IT and Development Centre).

The voting application can be downloaded from the elections website and may be used by any voter with internet access and Windows, macOS or Linux operating systems. No prior registration, geographical restrictions or maximum limit on the number of users is imposed. All that is required is an internet connection, an Estonian ID card and a card reader or mobile ID on a mobile device for authentication and signing. The voter confirms their identity using the ID card or mobile ID and is presented with the list of candidates. After the voter has made their choice, the application encrypts the vote using the public key of the internet voting system. The encrypted vote is signed with an ID card or mobile ID and the vote is sent to the vote collecting server. There, the vote is registered by a server service. The voter signature is verified and if the signature's certificates are valid, the voter is notified that the vote has been received and the vote verification QR code is generated in the voting application.

Each voter can verify that their vote has been 'cast-as-received' using a separate device (such as a smartphone) with a vote verification application (iOS or Android). Scanning the QR code with a mobile application will return a voter's pre-cast choice to the mobile app.

After internet voting has closed, the checksum of the electronic ballot box is generated and digitally signed by a voting collector manager before delivery to the State Electoral Office. Vote counting takes place on a computer disconnected from the internet, and votes are decrypted on a computer RAM disk instead of on a hard drive. The integrity of the system, the data and the voting results are verified by auditors using a separate auditing application. Other interested parties can write their own auditing application and verify the results themselves[82]. Only after the verification of system data has been concluded can the final voting results be signed off.

5.4.6 Communication campaign/awareness raising, including building voter trust and confidence

The State Electoral Office and State Information System Authority jointly conduct the e-voting voter-awareness campaigns. Awareness building focuses on three aspects:

1) cyber hygiene: safe digital handling of the digital identities (e-ID) and how to keep a voter's PC and software secure and up-to-date.

2) trust in internet voting: how internet voting works and how internet voting procedures and results are verified.

---

[82] For this purpose, the ballots which use homomorphic encryption are mixed before verification. This ensures that voting secrecy is maintained, and any interested party can access the mixed votes.

3) voter awareness and practical information: when, how and where to vote, reminding voters to check that their e-ID is working and that their PC operating system and e-ID software are up-to-date.

The transparency of the system and its procedures is essential in building voter trust. As required by law, the State Electoral Office's activities are public, as are the documentation and protocols of the internet voting system. All procedures should also be observable. The State Electoral Office offers training to observers including a run-through of all the internet voting procedures. The final step of the election preparation process is the 'official voting trial', held shortly before the elections, where auditors and observers verify: (i) the system for casting votes; (ii) that the encryption keys are working; and (iii) that poll results will be ascertained correctly. The same system and encryption keys are in use for the upcoming elections.

According to research by the Johann Skytte Institute of Political Science of the University of Tartu[83], during the 2019 parliamentary elections, 68.7 % of eligible voters indicated that they either 'highly trust' or 'trust' this voting procedure. This number is slightly higher among younger people, but internet voting in general seems to enjoy high levels of trust in Estonia regardless of age group. The highest trust level on average is recorded among people who have used this voting method, i.e. internet voters themselves, followed by conventional paper voters. The least trusting group mainly comprises abstainers.

While trust in internet voting is high, there is some degree of polarisation, whereby a large majority has very high trust levels and a small group has very low levels of trust, with hardly anyone in between. Over the years, this polarisation has been mitigated by paper-ballot voters switching to internet voting and then showing higher trust levels. The study concluded that eliminating polarisation entirely remains unlikely, as internet voting continues to be politicised by some political parties, which impacts strongly on their voters' perceptions[84].

Individual vote verification has increased confidence in internet voting for those Estonians who choose to verify their vote: those who are aware of the option of vote verification are more confident in internet voting than voters who are unaware of this option. This suggests that trust can already be increased by building and communicating about verification possibilities without a large uptake of this functionality among actual users[85].

5.4.7 Accessibility for people with disabilities and older people

Internet voting in Estonia is fully accessible to people with disabilities, since the website used for voting in the country complies with the web-accessibility standard required under the Web Accessibility Directive. This allows people with disabilities, including those using assistive technologies like screen reader software, to cast their vote independently.

Internet voting in Estonia is based on the principles of the web accessibility initiative, a series of recommendations drawn up by W3C, the main standards organisation for the World Wide Web. The web accessibility initiative develops strategies, guidelines, and resources to help make the web accessible to people with disabilities. Internet voting in Estonia is also based on JAWS (Job

---

[83] https://www.valimised.ee/sites/default/files/2021-10/Trust%20in%20Estonian%20Internet%20Voting.pdf

[84] Ehin, Piret; Solvak, Mihkel (2021). Party Cues and Trust in Remote Internet Voting: Data from Estonia 2005-2019. In: ed by Robert Krimmer et al. Electronic Voting: 6th International Joint Conference, E-Vote-ID 2021, Virtual Event, 5–8 October 2021, Proceedings (pp. 75-90). New York: Springer. (Lecture Notes in Computer Science; 12900)

[85] Solvak, Mihkel (2020). Does Vote Verification Work: Usage and Impact of Confidence Building Technology in Internet Voting. In: Krimmer, R. et al. 5th International Joint Conference, E-Vote-ID 2020, Bregenz, Austria, 6–9 October 2020, Proceedings (pp. 213-228). Springer. (Lecture Notes in Computer Science; 12455)

Access With Speech), a tool that converts text and components of the Windows operating system into synthesised speech, thus allowing people with visual impairments to access written information in audio format.

Estonia's voting application provides for the use of JAWS[86] screen readers, including assistive technology to help individuals with disabilities to use computers with ease. There are plans to introduce similar support for the macOS operating system. Internet voting also works as a universally available voting option for people unable to vote at the polling station. Should the voter wish to use a paper ballot, home voting is arranged for them on request.

Figure 5 Participation in Estonian local elections – 2021

| Status | Participation/non-participation | | | |
	Did not vote (%)	Paper votes (%)	Voted via internet (%)	Total
Employed	20.59	36.15	43.26	100.0
Studying	16.92	24.62	58.46	100.0
Retired	13.97	48.53	37.50	100.0
At home (with children or otherwise inactive on the labour market)	40.0	26.67	33.33	100.0
Unemployed	31.11	40.0	28.89	100.0
Permanently unable to work or disabled	33.33	31.11	35.56	100.0
Other	33.33	0	66.67	100.0

Source: Estonian internet voter study 2005-2021

5.4.8 Data protection and Council of Europe standards

Estonia's National Election Committee has issued technical requirements for internet voting to ensure compliance with fundamental voting principles. These requirements are based on the 2017 Council of Europe recommendations on e-voting. Before each election, the risk-analysis plans and risk-management plans are updated, and penetration tests are conducted on the system. Before each election, the voting system is audited via an ISKE security audit[87]n; as well as via a separate audit of internet voting procedures commissioned by the Ministry of Economics and Communications. The ministry also issues a separate elections cybersecurity assessment before each election.

Voter lists, including information on voter participation, are not public and voters can only check their own data. The voter's choice is protected by ballot encryption; before votes are counted, the voter identification data are removed from the ballots. Once a month has passed or all election complaints have finally been resolved, votes cast by internet and the key for opening these votes are destroyed. Personal voter data in the internet voting system are also destroyed, but anonymised voting logs remain available for research.

---

[86] Job Access With Speech (JAWS) is a computer screen reader software program.
[87] Three-level IT Baseline Security System ISKE; based on a German IT Baseline Protection Manual (IT-Grundschutz). Replaced by E-ITS (Estonian Information Security Standard) audit from 1/1/2022

5.4.9   Threats and vulnerabilities identified and mitigation measures

The vote-collecting services are hosted by Estonia's State Information System Authority[88]. The risk that these services could be subject to a distributed denial of service (DDoS) cyber attack is mitigated by using several sets of clustered servers situated at different physical locations. The voting application uses the HTTPS protocol over a TLS layer. To ensure that voters use the official voting application, its integrity can be verified by application checksums that are available on the State Electoral Office's website. The State Information System Authority also ensures round-the-clock availability of technology and cybersecurity teams, and it monitors all of Estonian cyberspace', in heightened readiness to intervene, during election week.

The impact of internet voting in Estonia has been scrutinised since its introduction in 2005[89]. One of the expectations for internet voting was that it would engage more voters and increase the number of younger voters. However, in Estonia, the positive impact of internet voting on voter participation has been shown to be negligible. The simplest explanation for this is that since there are so many ways to vote by ballot for a whole week, voters are not constrained by their choice of voting methods. In comparison, however, internet voting did promote increased turnout among Estonian voters abroad. The possibility to cast votes via the internet made the previous process, which involved either voting in an Estonian representation or ordering the ballot by post, easier and more accessible for voters resident outside Estonia.

5.4.10 Links to further information

Elections website: https://www.valimised.ee/en

Information System Authority: https://ria.ee/en

Riigikogu Election Act: https://www.riigiteataja.ee/en/eli/514122020002/consolide

ID card portal: https://www.id.ee/en/

5.4.11 Contact

State Electoral Office

www.valimised.ee

https://www.facebook.com/eestivalimised/

5.5 Online electoral registration in Ireland

5.5.1   Short description

The Irish government has committed to a broad range of electoral reforms, among them the modernisation of voter registration, and including options to register to vote online. With the commencement of parts of the Electoral Reform Act 2022 in October 2022, online registration is now provided in two ways, as set out below.

---

[88] The authority is the main partner of the State Electoral Office for hosting and maintaining all election information systems.
[89] M. Solvak and K. Vassil. E-voting in Estonia: technological diffusion and other developments over ten years (2005-2015). University of Tartu, 2016.

1. **Check the Register** – www.checktheregister.ie allows electors and potential electors to check their details and submit an online form to their local authority to register or update their details.

2. **Voter.ie** – www.voter.ie has been available in the Dublin region since 2019. It provides a self-service portal and public access to allow electors to check the register of electors, create, update or delete their voter registration through a change-request process. In addition to an online application form, Voter.ie facilitates the use of MyGovID – the Government's online authentication portal.

Both websites also provide downloadable paper forms for anyone who does not wish or is unable to use the online service.

5.5.2 Legal framework

Part 3 of the Electoral Reform Act 2022, enacted on 25 July, underpins Ireland's reformed registration process. The necessary provisions relating to electoral registration were introduced on 13 October 2022 under S.I. No 512 of 2022. The legislation provides for a registration process based on three different identity data checks, two of which involve online registration. In addition, the legislation includes a general provision for the use of electronic or digital means of submitting documents where facilities exist. The Act also provides for the development of a national shared electoral registration system, within which each local registration authority will continue to manage the register for its own administrative area. The national system will be available for all registration authorities to migrate to from 2025. In the interim, the existing systems supporting the electoral registration process have been updated to ensure compliance with the provisions in the Act.

5.5.3 Brief description of the software system and technology used

The three IT systems that registration authorities currently employ to help them meet their obligations around electoral registration have been designed to enable each local authority to meet all of the requirements set out in the legislation.

Both the 'Check the Register' website and the separate iReg system used by local authorities outside the Dublin region to administer registration are built on the Microsoft Windows operating systems platform, with Microsoft SQL Server databases in the back-end.

Voter.ie is a two-part hybrid solution which comprises a back-office system held within Dublin City Council's datacentre and a public-facing portal within the Microsoft Azure platform. The back-office system provides election management, voter management, correspondence, election book and reporting functions. The system is written in a combination of C+.Net, MVC, MS-SQL Server, and MS-SSRS. The front-end portal resides in Dublin City Council's Microsoft Azure tenancy. While the back-office and public-facing portal are currently integrated, the back-office is decoupled from the public-facing portal to protect the performance of the electoral registration system and to provide a security 'air gap'.

procurement of the new national electoral registration system began in September 2023. The proposed option is to strengthen and improve the current voter.ie system to meet the requirements of the national online electoral registration system. The technical infrastructure/architecture proposed in this option includes a full cloud solution (both front-end and back-end will be in the cloud).

To mitigate cybersecurity risks associated with a range of threats, the system will be developed and supported using industry best practice methodologies including the NIST cyber security framework, ISO27001 and the Cloud Alliance control framework. The system will also be the subject of an annual report to Ireland's independent Electoral Commission.

5.5.4   Testing methodology

ITIL, PMBOK and industry-standard methodologies will be adopted during the implementation and development of the national system and its operational support.

The standard 'waterfall' methodology will be adopted to ensure the successful delivery of the system, with the following core testing functions included:

- integration/system testing;
- unit testing;
- functional testing;
- usability testing;
- non-functional testing;
- performance testing;
- security testing;
- system unit acceptance testing.

5.5.5   Functional and operational flow

Below is a general outline of how requests to register/update details are currently processed.

Figure 6: General flow for applications to register/update details – voter.ie
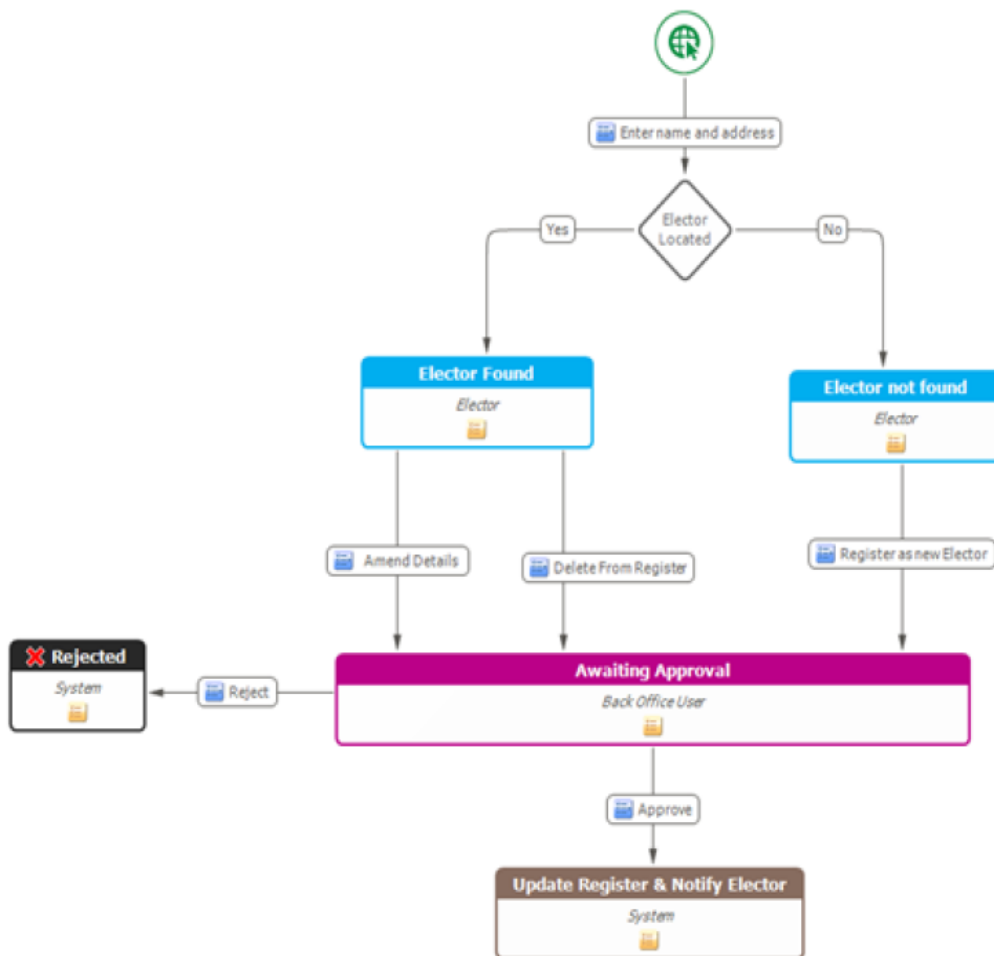
Source: Department of Housing, Local Government and Heritage of Ireland

While local authorities outside the Dublin region have a more manual process, it is nevertheless similar in overall flow to the above.

5.5.6 Communication campaign / awareness raising, including building voter trust and confidence

Before embarking on the reforms to the registration process a major public consultation process ran from 17 December 2018 to 15 March 2019. A significant awareness programme accompanied the consultation period to maximise reach and encourage a wide range of people to input. Submissions were received from a range of individuals, community and voluntary organisations, local authorities, public representatives, political parties and other stakeholders. A report on the consultation process was published.

Following commencement of the provisions, a major national public awareness campaign was launched in early November 2022. The purpose of the campaign was to raise awareness among the Irish public and to help registration authorities to encourage electors, both new and existing, to check and complete their information using their Personal Public Service Number (PPSN), post code and date of birth. A wide range of media platforms was used in the campaign, including conventional, social, and digital, to reach as wide an audience as possible. The material designed for the national campaign was also distributed to local authorities, and posters were supplied to a wide range of civil society organisations. Two further campaigns ran in June and November 2023, with some additional resources specifically focused on youth and older cohorts. Online information leaflets are available in a range of languages to ensure access to the relevant information for all.

5.5.7 Accessibility for people with disabilities and older people

Improving accessibility for all was a key aim of the policy reforms. Check the Register's accessibility statement can be consulted at https://www.checktheregister.ie/en-IE/accessibility. The checktheregister.ie website has been accessibility tested and all forms on the site are now fully accessible. The voter.ie website currently displays a compliance logo issued by the Web Content Accessibility Guidelines, another initiative of W3C the main standards organisation for the World Wide Web.

For those who do wish to use the online option or wish to apply for a special or postal vote, forms are available by downloading them from the checktheregister.ie or voter.ie websites or by requesting them from the relevant local authority. These forms are available in a fully accessible format.

In developing and simplifying the new forms to support the application process, the aim was to use clear, user-focused language. In pursuit of that objective, the department consulted with the National Adult Literacy Agency (NALA) on content.

5.5.8 Data protection and Council of Europe standards

As part of the process, compliance with the Council of Europe's guidelines is ensured in line with the commitment to deliver a safe and secure electoral registration system. Four key priorities guided the recent upgrades to Ireland's electoral system, and these priorities will remain priorities for the development of the national system. These four themes are: (i) the security and stability of the system, (ii) data protection; (iii) ensuring accessibility for all; and (iv) ensuring ease of use for all. Security (of data and system) and a human-centred approach were principles that informed the work on the updated versions of iReg, voter.ie and Check the Register.

5.5.9 Threats and vulnerabilities identified and mitigation measures

Potential risks such as cybersecurity and upscaling/loading were identified and relevant mitigation measures implemented following a security audit, which included penetration testing

as well as load testing. Steps were also taken to ensure that the systems could respond to potential surges in application numbers arising from awareness-raising measures.

5.5.10   Links to further information

Public information website: https://www.gov.ie/en/policy/61d9b3-local-government/#voting

Information leaflet: https://www.gov.ie/en/collection/897bd-information-on-the-register-of-electors-in-a-range-of-different-languages/

Check the Register (public-facing portal): www.checktheregister.ie

Voter.ie (public-facing portal): www.voter.ie

5.5.11 Contact

Franchise (Electoral Registration Modernisation) Section

——

Department of Housing, Local Government and Heritage

Custom House, Dublin 1, D01 W6X0, Ireland

——

Email : registerreform@housing.gov.ie

www.tithiocht.gov.ie

www.housing.gov.ie

5.6 Electoral Dispute Management (EDM) in Lithuania

5.6.1   Short description

The Electoral Dispute Management (EDM) functionality is an ICT solution designed to manage complaints, notifications, and contingencies in elections. Voters may submit complaints and notifications online to all EMB levels (Central Electoral Commission, constituency election commissions, polling station election commissions). EDM also allows the EMBs to register contingencies.

5.6.2   Legal framework

EDM functionality is part of the Central Electoral Commission's (CEC) information system, established by the Law on Management of State Information Resources[90]. The CEC information system has its own regulations approved by CEC Decision No Sp-246 of 28 November 2019[91].

Lithuania's CEC information system supports most aspects of the electoral process, including voter registration and identification, candidate registration, training for election officials,

---

[90] https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.415499/asr
[91] https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/511445c2127811eaad00dac7ebcb2435

campaign finance oversight, electronic counting of preferential votes, and the transmission of election results[92].

5.6.3   Brief description of the software system and technology used

EDM forms part of the module of electronic services within the 'Voter's Page' portal[93]. 'Voter's Page' is an integrated subsystem of the CEC information system designed to ensure electronic interactions between the CEC and voters, candidates and other electoral stakeholders. These interactions include: (i) e-signatures in support of candidates and political parties; (ii) e-submission of nomination documents; (iii) e-training; and (iv) voters' accounts where voters can find all relevant information about elections and their polling station. The CEC information system is browser-based and accessible only to authorised users via electronic identification. EDM's programming language is JAVA, the database is ORACLE, and the application is EgoDMS. It was developed by the private company iSense as a custom solution.

Figure 7 Electoral Dispute Management (EDM) functionality
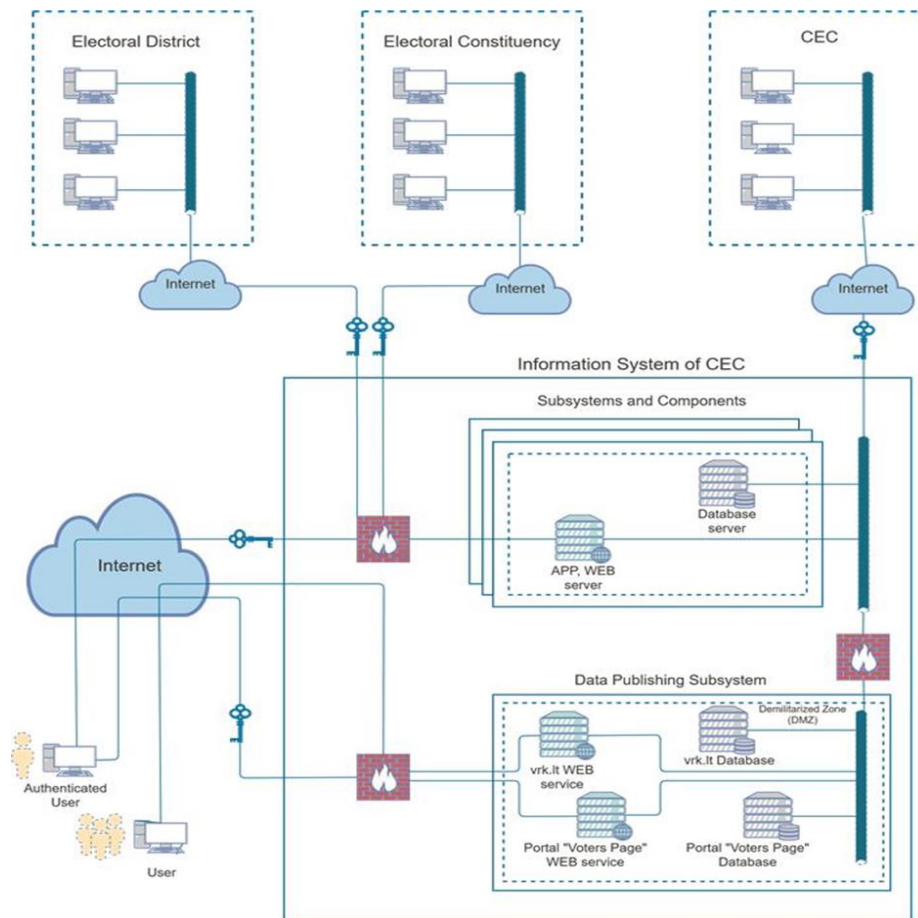
Source: Central Electoral Commission of Lithuania

5.6.4   Testing methodology

EDM was tested before it was brought into operation, firstly by the vendor and later by the CEC according to predefined test scenarios, which were described in the project management documentation. The scenarios covered a range of possibilities, for example, the chair of a municipal election commission receiving and registering a complaint. The test scenario checks

---

[92] 477730_0.pdf (osce.org)
[93] www.rinkejopuslapis.lt

whether all functionalities are operational: login, document registration form, notifications to users, and publication. An example of a programming error would be if not all notifications about the actions within EDM were delivered to the EDM users by email. Such programming errors, which were identified during testing, were included in the test report and subsequently rectified by the vendor. EMD was already used in two of Lithuania's mayoral by-elections in 2021 in the Trakai and Kelmė municipalities, where the municipal election commissions had to register complaints they received during the electoral period.

5.6.5   Functional and operational flow

EDM has the following functions:

- an authenticated user submits an online complaint or notification to the relevant election commission (CEC/constituency/polling station) by filling out a form with the following information: type, title, description, place, date, subject, type of election, type of election commission, etc.
- the complaint or notification is received and registered by the relevant election commission;
- the EDM administrator assigns a person to investigate the complaint or notification;
- the person responsible for the investigation examines a complaint or notification (during the examination EDM allows the registration form to be supplemented with additional information, files to be attached and a reply to be drafted).
- replies are sent via the system to the applicant;
- information about procedures is published on the CEC website and on the map displaying the number of complaints and notifications ascribed for each election commission;
- EDM has an interface with the document management system used by the CEC and transmits registration information to create an electronic document which is then registered in the document management system, thus avoiding duplicate registration.

5.6.6   Communication campaign/awareness raising, including building voter trust and confidence

A communication campaign on new EDM functionalities was conducted in 2021. It included a promotional video about the main functional features of EDM. This video was uploaded on the website of the CEC and on social media. At an online public event, the CEC unveiled all the functionalities created during the project, including EDM.

5.6.7   Accessibility for people with disabilities and older people

EDM is part of the 'Voter's Page' portal, which is accessible to visually impaired people as well as people with other disabilities. This portal has a special, adapted mode that enables people with disabilities to read the content of the website using the assistive software. The portal has a simple and user-friendly interface, and complies with the Web Content Accessibility Guidelines standard.

5.6.8   Data protection and Council of Europe standards

EDM is compliant with the 2022 Council of Europe guidelines on the use of ECT in electoral processes, because it is easy to understand and use for all voters and also accessible to voters with disabilities. It is available only to authenticated voters in Lithuania whose personal data are protected under the GDPR. An applicant may send a complaint or notification directly to the relevant election commission and will receive a reply through the same functionality. All

complaints and notifications that are accepted and examined by the EMBs will be published on the CEC website, ensuring transparency and data protection.

5.6.9 Threats and vulnerabilities identified and mitigation measures

Lithuania's National Cyber Security Centre (NCSC) is tasked with cybersecurity management of the overall CEC information system (VRKIS) which includes EDM. VRKIS safeguard procedures include: (i) monitoring for malicious activities; (ii) NCSC security clearance of staff; (iii) contingency planning; (iv) separation of access and duties; and (v) logging all activities, thus providing accountability. Safeguards against system failure include a business continuity plan (prepared by the CEC and tested by the vendor) as well as backup/archiving, both in line with national regulations and international standards[94].

Threats and vulnerabilities were tested before rolling out EDM. No major glitches were identified. The vendor was responsible for eliminating errors in the post-warranty period.

5.6.10 Links to further information

Central Electoral Commission website: https://www.vrk.lt/en/home

 'Voter's Page' website: https://www.rinkejopuslapis.lt/pagrindinis

Link to information about electoral legislation: https://www.vrk.lt/teisine-informacija

5.6.11 Contact

> Central Electoral Commission of the Republic of Lithuania
>
> State budget institution, Gynėjų st. 8, LT – 01109 Vilnius, Lithuania
>
> rinkim@vrk.lt

5.7. ICT solutions used in Romania to increase the integrity of elections

5.7.1. Short description

Romania uses several ICT solutions to improve the management of elections and increase their overall transparency. These ICT solutions include: (i) the electoral register first used in the 2014 European Parliament elections; (ii) the system for monitoring turnout and preventing illegal voting (SIMPV); and (iii) a tabulation system (SICPV).

5.7.2. Legal framework

The ICT solutions used in Romanian elections are regulated primarily by Law No 208/2015 on the election of the Senate and the Chamber of Deputies, as well as for the organisation and functioning of the Permanent Electoral Authority (PEA). The legal framework also includes several regulations issued by the PEA, such as PEA Decision No 36/2019 on the operation of the information system for monitoring turnout and preventing illegal voting, selection, and the appointment of computer operators of the electoral offices of polling stations, and the verification of correlations in the recorded tallies of voting results.

---

[94] 477730_0.pdf (osce.org)

5.7.3. Brief description of the software system and technology used

Romania's electoral register is a web-based, integrated information system with a centralised architecture. It is used to register voters, including voters abroad, and assign them to polling stations. It compiles information from various authorities, including the Ministry of the Interior, mayors and voters.

The register is consulted by users from each administrative unit in the country as well as by users from the PEA. This system ensures simultaneous access, allowing all administrative units to simultaneously enter and update data on voters and polling stations available at their level. It contains two main sections: a public section open to all voters, and a private section for the public authorities authorised to operate it.

The register's architecture is based on three levels that can each be updated and replaced independently depending on user needs or technological requirements. The 'upper' level of the system is represented by the presentation layer, which shows the portal and communicates with the other levels through the results shown. The second level, known as 'app', is also the app's logical level and controls app functionalities. The third level is the data level, which is comprised of database servers on which information is stored and retrieved. This level stores data independently from the app servers and from the logical level in order to improve scalability and performance.

The electoral register's logical architecture is structured as follows:

• web server and apps server, both of which integrate the business services of the platform and ensure the integration of all system components;

• web portal available in the public system;

• database;

• business intelligence used for data interrogation and manipulation;

• external integration used in the form of web services available for access by other government apps;

• authentication module;

• server protection – antivirus;

• proactive monitoring and protection for servers;

• virtualisation module that improves usage performance of available hardware;

• client work stations from which end users have access to information system services via a web browser;

• external systems that access the web services available through the integration module.

In connection to the electoral register, the PEA introduced SIMPV and SICPV. While they address different electoral aspects, they also work jointly to deliver credible results. As well as verifying voters, SIMPV also allows: (i) audio and video recording of the vote-counting process; (ii) the creation and storage of results protocols, including scans; (iii) the checking of data correlations in the results protocols; and (iv) the transmission of results to SICPV. Based on SIMPV, Romania's Central Electoral Bureau reports disaggregated turnout data throughout polling day and begins publishing results for each polling station shortly after the polls are closed. Data from SIMPV are transmitted to SICPV, which tallies the election results while also allowing the publication of scans of the original results protocols, thus increasing the process' overall transparency.

Furthermore, to guarantee data integrity a block-chain solution for SIMPV and SICPV transactions was also implemented.

To visualise the block-chain, a new app structured over three pages was developed. It comprises: (i) a guard page containing the list of most recent blocks; (ii) a graphic display of most recently loaded data in blocks; and (iii) a snapshot of the latest data to be collected before being closed in a new block. The second page contains details of a block and transaction list, and the third page shows the transaction details.

5.7.4. Testing methodology

Performance testing takes place at the initial launch and after software or hardware component upgrades. Further security tests are conducted on a monthly/quarterly basis and after software upgrades. Additionally, all functionalities available in the user interface are tested by users according to a test plan.

The methodology used for assessing the security level of the ICT infrastructure is based on best practices in the field and involves a security classification system following identification of existing vulnerabilities in the system using Tenable's Nessus proprietary vulnerability scanner. The vulnerability risk level is based on the common vulnerability scoring system.

The functionalities available in the user interface are all tested by users according to a test plan.

Given that subsystems are hosted by the main ICT infrastructure, performance testing at launch and after updates is also carried out for the subsystem.

Performance, security, and high availability testing were performed before entering the production phase. Performance testing was carried out using the Jmeter software tool. All functionalities available in the user interface were tested by users according to a test plan.
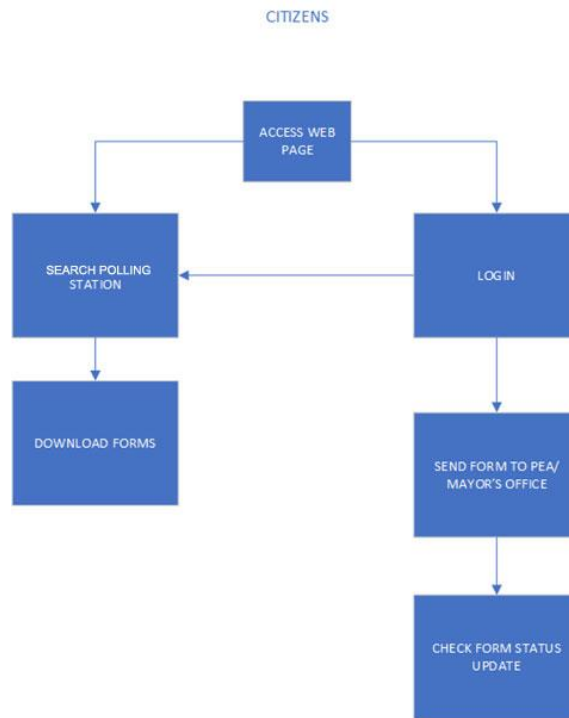
5.7.5. Functional and operational flow

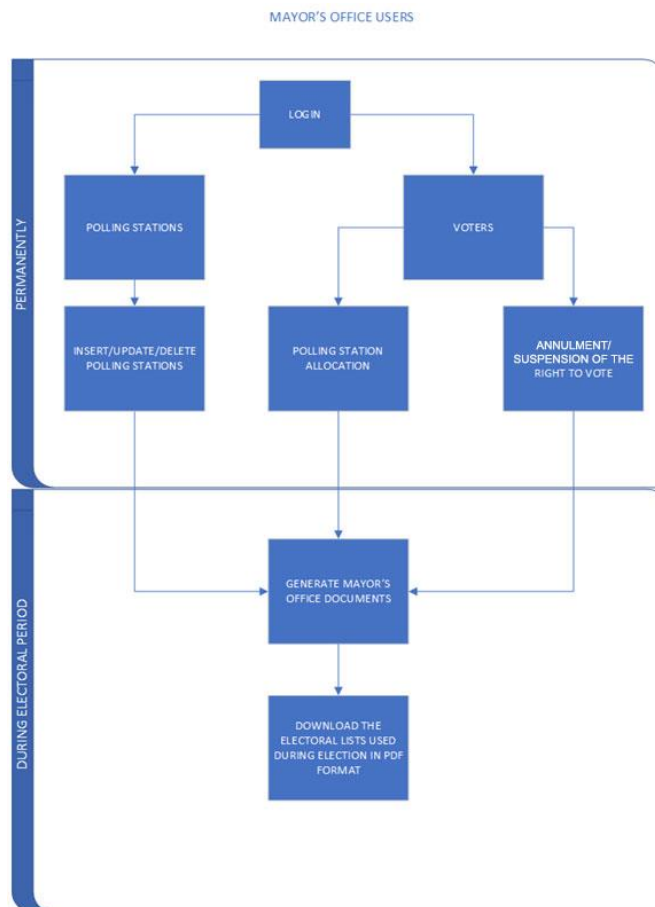The functional and operational flow includes the steps illustrated as follows.

The figure below illustrates the functional and operational flow for PEA users:
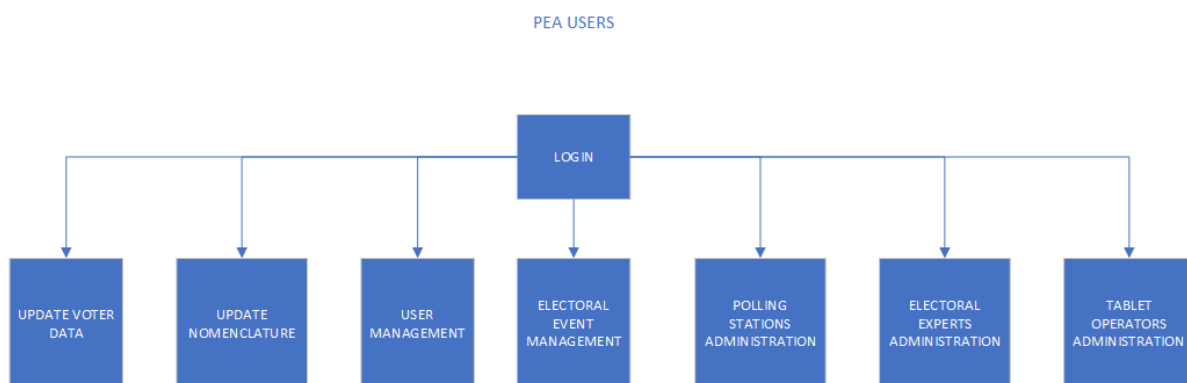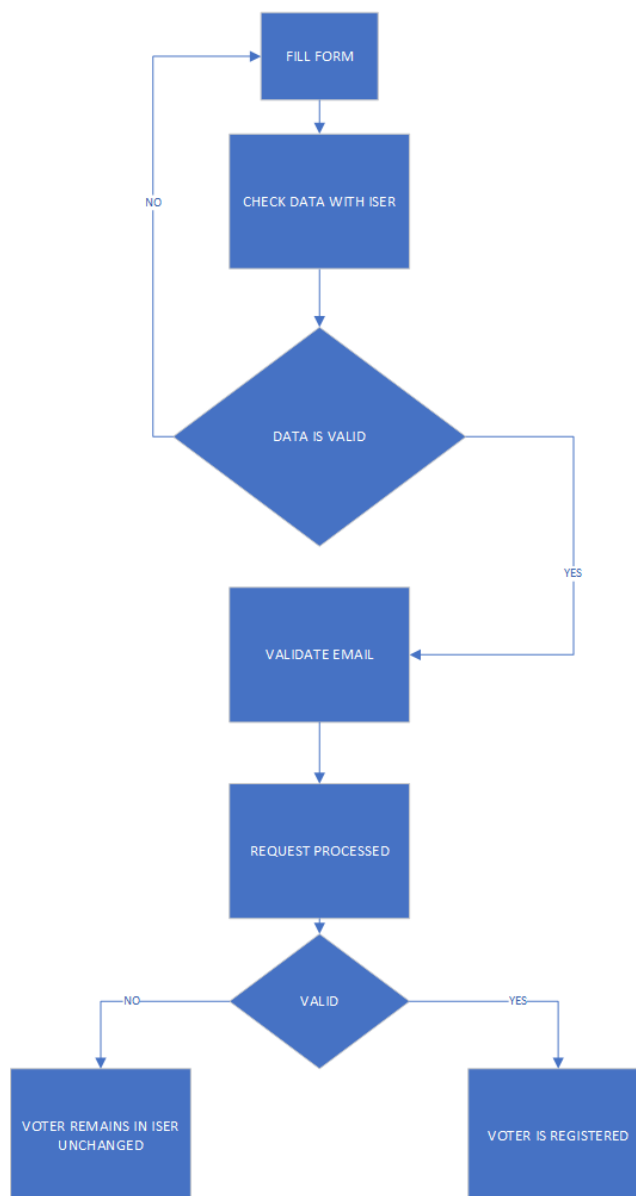

The figure below illustrates the functional and operational flow for voters located in Romania:

The figure below illustrates the functional and operational flow for the staff of mayors' offices:

The figure below illustrates the functional and operational flow for voters resident abroad:

5.7.6. Communication campaign/awareness raising, including building voter trust and confidence

At the beginning of each month the PEA issues a press release on the total number of voters compared to the previous month. The differences from month to month are the result of ongoing operations performed in Romania's electoral register. The differences are in turn broken down into a number of categories such as: (i) the number of voters by age group; (ii) the number of voters living in different environments (urban/rural); (iii) the number of voters in each city; and (iv) the number of voters in the country and outside it (for Romanian voters resident abroad). The press release is also shared on the PEA's official Facebook page.

To increase both the use of postal voting, as well as turnout among Romanian voters resident abroad, the PEA conducts online and offline public information campaigns. These campaigns are aimed at raising awareness about online registration[95] for postal voting or for voting at a polling station closer to home. These information campaigns encompass: (i) regular press

---

[95] Available at: www.votstrainatate.ro

releases; (ii) public statements from the PEA's president; (iii) media briefings; (iv) offline documentation points; (v) in-person and online meetings with Romanian ex-pat communities; and (vi) information videos produced by the PEA and promoted via social media and other channels.

5.7.7. Accessibility for people with disabilities and older people

The PEA has set up an online system to help voters locate their assigned polling station. Thus, a person can enter their name and personal identification number on the www.registrulelectoral.ro website (a component of the electoral register) and on the next page they will find their polling station's reference number and address. The PEA intends to develop an additional module in the 'Take me to the polling station' section of this website exclusively for people with disabilities. This section of the website for people with disabilities will use text-to-voice technologies to guide voters (people with disabilities) to the nearest accessible polling station where they have the right to cast their vote.

On the announcement of election results, the PEA also has a webpage (https://prezenta.roaep.ro/) on which it is possible to monitor the partial and final results of elections in real time. In 2022, the PEA's www.roaep.ro website was made accessible to people with visual impairments, by allowing text enlargement, text reading, greyscale scaling, increased contrast, negative contrast, light background, underlining of links, and the transforming of fonts to make them easier to read.

5.7.8. Data protection and Council of Europe standards

The PEA respects data protection principles through design and data minimisation when processing personal data, including processing by means of ICT solutions.

On Guideline 6, when referring to Article 6(1) of the Council of Europe Convention for the protection of individuals with regard to the processing of personal data (ETS No 108), personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or intimate activity will not be processed automatically or stored by the PEA or any other state authority.

On Guideline 7, the PEA and the other institutions involved in the electoral process constantly inform voters and other interested parties about the aims of data processing, stating that the data will not be used to track individuals for any other purpose, i.e. the payment of taxes or the legality of residence abroad.

5.7.9. Threats and vulnerabilities identified and mitigation measures

At the service infrastructure level, PEA solutions are built on a multi-level modular architecture in which, for security reasons, only adjacent modules can communicate with each other (level one with level two/level two with three, etc.). To ensure availability each tier has a cluster structure (active-active or active-passive).

The systems are hosted in the TIER 3 data centre, to which only designated technical and security administrators have access.

Many firewall devices are used to monitor traffic and check, for each generated data session: (i) the source IP address; (ii) the destination IP address; (iii) the port on which the communication takes place; and (iv) the integrity and legitimacy of the open session. To ensure redundancy, firewall equipment is configured in an active-passive cluster architecture.

The system connects to the internet through a redundant firewall solution capable of ensuring greater security and availability.

PEA also implements effective and rapid cybersecurity measures, using both automated mechanisms and technical operations in real time around the clock.

5.7.10. Links to further information

- www.roaep.ro
- https://prezenta.roaep.ro
- Law-no.-208.pdf (roaep.ro)

5.7.11. Contact

> - Permanent Electoral Authority of Romania (PEA) – registratura@roaep.ro;
> - Department of legislation, election dispute resolution, and liaison with Parliament and the European Union:

5.8 ICT solutions used in electoral processes in Czechia

5.8.1. Short description

Electoral technologies are used variously in Czechia during all phases of the electoral cycle. IT is mainly used in two phases: (i) when tallies of voting results are compiled by district election commissions ('voting operations' phase); and (ii) when the data obtained are transferred from district election commissions to the central database for the subsequent calculation and presentation of election results ('election results' phase). The principles of impartiality, transparency and security are respected in both these phases.

Current legislation in Czechia does not provide for the use of digital technology directly for voters to cast their votes, either remotely (e.g. via the internet) or at a polling station (e-voting machine). The votes are therefore cast in paper form and counted manually by the individual district election commissions (no scanning technology is used).

5.8.2. Legal framework

The use of digital technologies in elections is currently enabled by general electoral legislation in Czechia, and the use of ICT is addressed in several election-related laws[96]. A project is currently ongoing to unify legislation under a single electoral act (draft act on election administration, see below in section 4.8.9). The rules on the use of ICT are set out according to the specific stage of the electoral cycle in which they are used. The Czech Statistical Office (CZSO) produces for each election an up-to-date internal guidance document, *'Technical project for the collection, processing and presentation of election results'*, and updates an internal guidance document, *'Basic principles for the safe use of technology in elections'*. These two documents set out the principles and methodology for the use of ICT in elections to ensure the safety of election processing.

---

[96] Local Municipal Election Act: https://www.senat.cz/xqw/xervlet/pssenat/webNahled?id_doc=2888&id_var=2888; Parliament Election Act:
https://www.zakonyprolidi.cz/cs/1995-247; European Parliament Election Act:
https://www.zakonyprolidi.cz/cs/2003-62 and Act of Law 247/1995 Coll. on elections to the Parliament of the Czech Republic; President Election Act: https://www.zakonyprolidi.cz/cs/2012-275; Regional Municipal Election Act: https://www.zakonyprolidi.cz/cs/2000-130

5.8.3. Brief description of the software system and technology used

The software for processing votes and transferring data from collection points to the CZSO central office was created by the CZSO in cooperation with an external supplier. CZSO hardware is used with the support of the communication infrastructure of supplier companies. All technical means used in the processing of election results are secured by full redundancy. The software used is designed in such a way as to ensure parallel processing (load balancing) and automatic continuation of processing in the event of failure of one of the components secured in this manner. All data are centrally processed using the ORACLE database system.

5.8.4. Testing methodology

The cybersecurity of election processing at the CZSO level is addressed by an internal guidance document produced by the CZSO. Other CZSO materials also address cybersecurity, including internally produced materials on crisis scenarios, which determine the processing procedure in the event of non-standard situations. In matters of cybersecurity, the CZSO cooperates with relevant institutions (Ministry of the Interior and the National Cyber and Information Agency) as well as with service providers. Penetration tests are regularly carried out, and processing tests are organised to verify the functionality and safety of all processes, especially digital technologies.

5.8.5. Functional and operational flow

District election commissions may use an offline computer election program with a built-in system of interactive mathematical-logical checks to alert the district election commission to potentially incorrect information when compiling a record of constituency voting results (i.e. recording of manually summarised results).

The processing of election results involves several steps. Firstly, voting results are electronically transferred from the district election commissions to a central processing hub via the Czech Statistical Office (CZSO) collection point. Representatives of the district commissions then travel to the CZSO's physical' collection point with a signed record and electronic record on a flash drive (over 90 % containing exported data with voting results from a computer program). After summarising the results for all constituencies, the election results are ascertained (and mandates divided) at the level of the central database. Detailed records (full and partial) of the election results are then generated.

This is now a standard form of digital processing of election results (personal transmission of manually recorded results in polling stations to the central state administration body, which then: (i) summarises the results; (ii) calculates the distribution of seats; (iii) publishes election results in the presentation system on the website; and (iv) forwards the results to the State Electoral Commission for approval). The presentation system of election results also uses a cloud solution.

The CZSO is setting up a protected transmission network in cooperation with external companies. The transmission network users are the CZSO central office and computers at collection points. The transmission network is protected between clients and the CZSO central office by creating a virtual private network (VPN). Remote clients log in to the transmission network using ADSL lines through the connection provider. Connection is only possible from pre-defined locations. A username and password are required to log in to the VPN.

5.8.6. Communication campaign/awareness raising, including building voter trust and confidence

The election department of the Czech Ministry of the Interior and the CZSO have produced several instructional videos that describe the entire election process, from voter verification to the voting process and the counting of election results. These videos are publicly available to voters and serve as supplementary study materials for election commissioners. At the same time, the CZSO has created several infographics to combat misinformation about election procedures.

The Czech Ministry of the Interior also publishes information for voters on its website. Election results are published on the CZSO website (https://volby.cz/index_en.htm) immediately after they have been transferred to the central online database. Members of the district election commission can immediately verify the conformity of the election results with the signed records submitted at the CZSO collection point, and members of the public can monitor results down to the lowest territorial (constituency) level. Results are permanently maintained online.

5.8.7. Accessibility for people with disabilities and older people

Before the election, the Czech Ministry of the Interior always provides voters with information on its website, which also contains guidance for voters with disabilities[97]. The Czech Ministry of the Interior website also provides: (i) information in sign language for voters with hearing difficulties; (ii) electronic previews of ballots usable by visually impaired people; and (iii) information written in simple language for people with mental impairments. This information is referenced using the QR code on the voter leaflet distributed with ballot papers. The current electoral system does not have any special IT tool to increase accessibility to elections for voters with disabilities or older people. However, the proposal for a new election management information system (see below) should do much to simplify the entire election process for this group of voters.

5.8.8. Data Protection and Council of Europe standards

In general, all processes during the preparation and holding of elections in Czechia are in accordance with the GDPR. Any changes or the introduction of new innovations are accompanied by a gradual change in legislation to preserve and safeguard all aspects of free and democratic elections (universal, free, equal suffrage, secret ballot, transparency, etc.).

5.8.9. Threats and vulnerabilities identified and mitigation measures

The current election administration is decentralised at the regional level, which can cause problems with the transfer of information and data. Therefore, the Czech Ministry of the Interior has prepared a new draft act on election administration, which would extensively digitise certain electoral administrative procedures, and could potentially improve the entire election process. The law is awaiting discussion.

The law would create an information system for election administration, as part of Czechia's critical infrastructure. This information system for election administration should become a new, unified information background for administrative activities in election calendars. In addition, the public interface of the system will enable access for individuals to electronic filing and ensure that the general public is kept informed, including via the publication of statutory documents at various stages of the electoral process.

---

[97]   Published in accordance with the Association for the Support of People with Mental Disabilities.

The election management information system will include four main components as set out below.

1. A central list of voters, replacing today's approximately 6 500 partial voter lists kept by municipal authorities.

2. A register of candidate lists, built on the possibility of using electronic candidate lists. It will facilitate the verification of candidate data and simplify communication between candidates and registration authorities.

3. A register of district election commissions, a tool that will allow electoral parties to delegate their representatives to district election commissions electronically.

4. An e-Petition tool, enabling the online creation of – and support for – electronic petitions for independent candidates using a guaranteed electronic identity. This option will exist in parallel with the possibility of submitting a paper petition.

5.8.10. Links to further information

Department of Elections official website: https://www.mvcr.cz/volby/.

CZSO official website: https://www.czso.cz/csu/czso/home

Government official website: https://www.vlada.cz/en/

Ministry of the Interior (legislature) official website: https://www.mvcr.cz/web-legislativa.aspx

5.8.11. Contact

> Elections Department of the Ministry of the Interior of the Czech Republic –
>
> Secretariat of the State Electoral Commission: volby@mvcr.cz

6. Final considerations

The main arguments for introducing e-voting and ICT solutions, including internet voting, are: (i) to facilitate voting and make it people-friendly; (ii) to encourage the trickle-down effect of the digitalisation of many other sectors and activities in society; and (iii) to improve the management of elections by making vote counting in particular less labour-intensive and potentially faster[98].

E-voting raises a number of issues, such as how to ensure free and secret ballots or how to ensure a reliable and secure electoral process. The practices presented in this compendium are intended to support Member States when dealing with such issues. They address topics such as: (i) internet voting; (ii) the use of voting machines and the use of ICT in voter registration; (iii) the management of complaints, notifications, and contingency reports; (iv) the verification of voters' eligibility; (v) the prevention of multiple voting; and (vi) the tabulation of election results.

---

[98] *2023 Study on E-Voting practices in the EU - https://commission.europa.eu/document/23076478-987e-4dea-b9ef-df5e0dfd6cd2_en*

They also include examples of testing methodologies, communication and awareness-raising campaigns, measures to ensure accessibility, and measures to mitigate threats and vulnerabilities.

A key finding of this compendium is that the introduction of e-voting and other ICT solutions in electoral processes needs to be accompanied by robust measures addressing security risks and ensuring compliance with data-protection requirements. Moreover, the identification of these accompanying measures should be part of the process from its earliest design phase[99]. In order to provide strong safeguards, identifying the specific challenges at stake represents an indispensable first step towards the implementation of e-voting solutions.

The introduction of e-voting should also ensure inclusiveness. Digital voting systems affect different types of voters in a variety of ways. For instance, research shows that people who are less comfortable with the use of technology (such as older people, or people with learning and cognitive disabilities) may find e-voting machines more intimidating and anxiety-inducing than most other voters[100]. In addition, for some first-time electors voting is something which they may wish to experience at a polling station. From this perspective, internet voting should be considered as an optional alternative to the polling station, not as a replacement for it.

People with disabilities may also be affected in different ways by e-voting options compared with the rest of the population. Remote and accessible voting alternatives may increase the possibilities for people with disabilities to exercise their voting rights effectively, in particular for voters with reduced mobility. At the same time, such options should not replace initiatives aimed at making conventional voting at polling stations more accessible to someone with a disability. This is because people with disabilities should also be able to choose their preferred method of voting, and because the act of voting itself is a key moment of integration and equality[101].

Drawing on the practices described in this compendium, when opting to introduce voting machines in their electoral process Member States could consider the following:

- seeking broad consultations involving independent bodies and experts, including scientific advice when it comes to the choice of options and settings;
- ensuring effective testing and auditing;
- providing clear and easy-to-understand public information, which should also be accessible to people with disabilities, along with the necessary support at all levels, including locally;
- making the use of ICT in elections easily accessible and user-friendly, and ensuring the technical possibilities for the constant improvement of accessibility to e-voting solutions for people with disabilities;
- ensuring that no state, region or municipality is in a situation of long-term electoral dependency on a specific private provider;
- ensuring adequate safeguards, including respect for data protection requirements, measures supporting confidentiality of the vote and protection against cyber risks;
- ensuring the existence of a protocol where an individual identifies an error to protect the secrecy of the vote;

---

[99] In line with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).
[100] *Ibid.*
[101] *Ibid.*

- ensuring that election officials receive appropriate training.

In any case, Member States should consider accompanying the use of any form of e-voting in voter-facing elements with specific monitoring, including accessibility for people with disabilities and equality between voters who use e-voting and those who do not.

Finally, when Member States decide to introduce internet voting, in addition to the important safeguards mentioned above they might also consider:

- introducing internet voting as a complementary voting method (i.e. polling stations continue to be offered as an alternative for people who wish to vote in person);
- relying on secure digital identification;
- and introducing specific measures to protect voters against potential coercion, such as the right to regret one's vote on election day (i.e. that it is possible to change one's vote until polling day).