Warsaw, 17 June 2025
Opinion-Nr.: ELE-EST/527/2025

OPINION ON THE REGULATION OF INTERNET VOTING

ESTONIA

This Opinion has benefited from contributions made by Ms. Ardita Driza Maurer, a Legal expert in the regulation of use of ICT in elections, Ms. Marla Morry, an International Lawyer and Legal Expert and Ms. Beata Martin-Rozumiłowicz, global electoral and ICT expert.

Based on an official English translation of the *Riigikogu* Election Act.

OSCE Office for Democratic Institutions and Human Rights

Ul. Miodowa 10, PL-00-251 Warsaw
Office: +48 22 520 06 00, Fax: +48 22 520 0605
www.legislationline.org

EXECUTIVE SUMMARY AND KEY RECOMMENDATIONS

On 17 September 2024, the Second Vice-President of the *Riigikogu* (Estonian Parliament), Mr. Arvo Aller, submitted a request to the OSCE Office for Democratic Institutions and Human Rights (ODIHR) to review the legislative framework governing internet voting in Estonia's parliamentary, local, and European Parliament elections. The Opinion and the analysis presented herein are a response to this request.

Internet voting has been used in Estonian elections for over 20 years. Over time, it has gradually become the most widely used voting channel in the country. It benefits from popular support and ODIHR has found in previous observations that "internet voting continued to enjoy a generally high level of public trust, owning to the transparency of the system…" It also found that "the internet voting process was organized professionally and transparently, with due attention to accuracy and security of the underlying systems, but with some technical difficulties". Nevertheless, political divisions over internet voting persist.

On 24 May 2024, amendments to the *Riigikogu* Election Act (REA) were adopted to the legislation in compliance with judgements of the Supreme Court from 2019 and 2023, which called for internet voting to be further regulated at the legislative level. These rulings emphasized the need for clear organisational, procedural, and substantive legal provisions to uphold legislative oversight and public trust in the electoral process.

The amendments mark a positive step towards greater legal coherence. They also take into account some of the principles developed by the Council of Europe in its various Recommendations on e-voting and ICT. In particular, the amendments make electoral principles such as universal, secret, and secure elections detailed requirements applying to internet voting. These represent an important modification of the REA in that they introduce a level of stability not previously offered by lower-level regulations. In another development, they consolidated and enhanced the existing provisions for cybersecurity.

Consultations on the 2024 amendments were held in which the government, parliament, political parties, and citizens could provide inputs. There was a lack of discussion, however, on how electoral principles should be interpreted in the context of internet voting.

Considering REA, as amended in 2024, and the broader legal framework governing internet voting, this Opinion provides several recommendations concerning the structure, content, and procedures for establishing legal and technical requirements for internet voting in line with international standards and good practice. The Opinion acknowledges that, like other voting channels, internet voting cannot fully and simultaneously satisfy all applicable electoral principles. While internet voting faces inherent challenges related to the principle of secrecy the legislation and practice in Estonia has worked to address this particular challenge. It is up to the Estonian Parliament to garner broad political and public support and determine how constitutional principles should be balanced in the context of internet voting and to define the corresponding legal requirements. ODIHR considers that inclusive, transparent, and in-depth discussions—leading to a consensual definition of the relevant legal and technical standards—are essential for fostering shared understanding within Parliament

and society and, ultimately, for continuing to build broad trust in internet voting as a credible voting method.

More specifically, ODIHR makes the following key recommendations to further enhance the internet voting regulatory framework's compliance with international principles and standards:

A. To introduce any future substantial modifications to the legal framework governing internet voting only following broad-based consultations and demonstrable support within Parliament and among the public, in order to enhance the legitimacy of the law and strengthen public confidence. Given the technical complexity of internet voting, such discussions should meaningfully involve a representative group of experts, including academia and civil society experts. [para. 42].

B. To further develop the legal requirements that implement the electoral principles of universality, equality, secrecy, and free exercise of voting rights in the context of internet voting. [para. 44].

C. To further strengthen the existing safeguards of the right to cast an internet vote freely and in secret, additional measures could include continuous voter education on these principles, clear instructions at the time of voting emphasizing the requirement to vote in private, and introduction of a mandatory declaration confirming that the vote is cast in secret and without coercion. [para. 46].

D. To explicitly oblige in the law the National Election Committee (NEC) and State Election Office (SEO), assisted by the Information System Authority (RIA), to monitor for potential breaches of the e-voting system and to introduce an explicit requirement for post-election audits to determine if any breaches occurred, specifically those related to secrecy of the vote in cases where group voting or voting in a sequence using the same device may be suspected. [para. 47].

E. To establish in the election law clear and objective criteria for decisions by the National Election Committee (NEC) not to initiate, to suspend, or to terminate electronic voting, or to declare its results invalid. Furthermore, it is recommended that clear conditions are legislated under which the NEC may decide to introduce or discontinue the use of mobile devices for internet voting. [para. 48].

F. To further clarify and develop the technical, organisational, security, and control requirements that give effect to legal provisions on internet voting, ensuring they continue to reflect state-of-the-art technology standards and international good practice. These requirements should be defined and regularly updated through a transparent and inclusive process, incorporating input from a representative group of experts, including academia and civil society experts. [para. 57].

G. To explicitly define in the REA all types of control and oversight mechanisms required for the internet voting system in place and related procedures, and to ensure that such controls are carried out by independent bodies. The applicable regulations should aim to reflect state-of-the-art technology and align with international good practice. [para. 58].

H. To clarify in the REA which forms of control may also be carried out by members of the interested public, such as qualified citizen observers and national or international experts, and to define the transparency measures necessary to enable such public oversight. These measures should aim to reflect state-of-the-art technology and align with international good practice. [para. 59].

I. To define in the REA the legal requirements for individual verifiability and its associated coercion-resistance measures, as well as for universal verifiability. This should include specifying who is entitled to conduct universal verifiability checks, taking into account the characteristics of the voting system. Additionally, consideration should be given to the conditions under which observers may be involved in observing such verifiability checks. [para. 65].

J. To consider introducing legislation that establishes the right and procedure for lodging complaints regarding internet voting related irregularities identified by observers, including the possibility for such complaints to be filed in the public interest. In this context, the legislator should also address the specific complexities of internet voting when determining appropriate deadlines, evidentiary requirements, and procedures for the submission, examination, and resolution of such complaints and appeals. [para. 68].

K. To consider updating criminal law provisions to establish offences and dissuasive, proportionate sanctions specific to all stages of the internet voting process [para. 69].

These and additional Recommendations, are included throughout the text of this Opinion, highlighted in bold.

As part of its mandate to assist OSCE participating States in implementing their OSCE human dimension commitments, ODIHR reviews, upon request, draft and existing laws to assess their compliance with international human rights standards and OSCE commitments and provides concrete recommendations for improvement.

TABLE OF CONTENTS

I. INTRODUCTION

1. On 17 September 2024, the Second Vice-President of the Estonian Parliament (*Riigikogu*), Mr. Arvo Aller, presented a request to the OSCE Office for Democratic Institutions and Human Rights (ODIHR) to provide a legal opinion on election legislation related to the use of internet voting in Estonian parliamentary, local and European parliament elections ("the request").

2. On 13 January 2025, ODIHR responded to this request, confirming the Office's readiness to prepare a legal opinion on the compliance of the internet voting legislation with international standards and OSCE human dimension commitments. In this Opinion, the terms 'electronic voting', 'e-voting' and 'internet voting' are used interchangeably, as they refer to the same voting method in the Estonian context. In line with ODIHR's methodology, this Opinion does not respond to the request's explicit question of whether it is "justified and safe" to continue using the Estonian electronic voting system under the current legal framework but discusses the implementation of key election principles related to internet voting, existing safeguards and where necessary how those safeguards could be made explicit in the legislation. ODIHR notes that decisions related to the use of electronic voting remain within the competence of the State.

3. In addition to its desk review, ODIHR held meetings with various electoral stakeholders, including representatives of Parliament, the National Electoral Committee (NEC), the State Electoral Office (SEO), the Ministry of Justice, all political parties represented in the *Riigikogu*, the Supreme Court, third party providers, civil society organizations, academics, and independent experts on 11-13 February and online on 18-19 February 2025.

4. This Opinion was prepared in response to the above request. ODIHR conducted this assessment within its mandate to assist the OSCE participating States in the implementation of their OSCE commitments. ODIHR staff and experts stand ready to present and discuss the Opinion's main findings and recommendations with all relevant stakeholders.[1]

II. SCOPE OF THE OPINION

5. The Opinion does not constitute a full and comprehensive review of the entire legal and institutional framework regulating elections in Estonia. It examines only the primary and secondary legislation governing internet voting.

6. The Opinion and the legal analysis presented herein is based on international and regional human rights and rule of law standards, norms and recommendations, and relevant OSCE human dimension commitments. The Opinion highlights, as appropriate, good practices from other OSCE participating States.

7. The recommendations put forward in this Opinion aim at enhancing the legal framework for internet voting in Estonia to clarify the safeguards and procedures in place that ensure the

[1] In paragraph 25 of the 1999 OSCE Istanbul Document, OSCE Participating States committed themselves "to follow up promptly the ODIHR's election assessment and recommendations".

implementation of internet voting is fully in line with relevant OSCE commitments and international standards. The recommendations should be read in conjunction with ODIHR's past recommendations in its election observation reports that remain to be addressed.[2]

8. While the request for this Opinion states certain concerns with the constitutionality of Estonia's legal framework for internet voting, ODIHR notes that the constitutionality of States' legislation falls under the exclusive purview of the national court empowered to examine constitutional matters. As such, this Opinion focuses on examining the applicable legal framework from the perspective of international norms and good practices.

9. In preparing this Opinion, the relevant legislation and other documents related to internet voting in Estonia were considered. This primarily includes the Constitution, the *Riigikogu* Election Act (REA), and the regulations issued by the National Election Committee (NEC). The Local Government Council Election Act, the European Parliament Election Act, and the Referendum Act reference the REA in terms of the organization of electronic voting and, thus, did not need to be considered separately. A wide variety of documents reviewed were translated unofficially, except for the Constitution, REA and other election laws, which are officially translated and published. Therefore, errors from translation may result. Should this Opinion be translated into another language, the English version shall prevail.

10. ODIHR would like to stress that this Opinion does not prevent ODIHR from formulating additional written or oral recommendations or comments on respective subject matters in Estonia in the future.

11. The following abbreviations are used: E2EV (end-to-end verifiability), EMB (Elections Management Body), NEC (National Electoral Commission), MJD (Ministry of Justice and Digital Affairs), REA (*Riigikogu* Election Act), RIA (Information System Authority), SEO (State Electoral Office), and SLA (Service Level Agreement).

III. LEGAL ANALYSIS AND RECOMMENDATIONS

3.1. Relevant International Human Rights Standards and OSCE Human Dimension Commitments

12. The main relevant international standards and best practices related to the Draft include:

- Paragraph 6 of the 1990 OSCE Copenhagen Document, which stipulates the free expression of the will of people through periodic and genuine elections and the respect for the rights of citizens to take part in the governing of their country either directly or through freely chosen representatives and Paragraph 7 that underscores the universal and equal suffrage of the adult citizens.
- International Covenant on Civil and Political Rights, Article 25 and General Comment 25 (11), "[s]tates must take effective measures to ensure that all persons entitled to vote are

[2] See previous ODIHR election observation reports on Estonia. See also ODIHR's repository of all recommendations, which also notes the status of implementation of prior recommendations.

able to exercise the right." Other international obligations and standards for democratic elections, such as those found in the 1950 European Convention on Human Rights, and Council of Europe (CoE) documents also apply. Of specific relevance are the Council of Europe Committee of Ministers Recommendation CM/Rec(2017)5 on standards for electronic voting, adopted on 14 June 2017, and the Council of Europe Committee of Ministers Guidelines CM(2022)10-final on the use of information and communication technology (ICT) in electoral processes, adopted on 9 February 2022.[3]

- International Convention on the Elimination of All Forms of Racial Discrimination, Article 5c, "states Parties undertake to prohibit and to eliminate racial discrimination in all its forms and to guarantee the right of everyone, without distinction as to race, color, or national or ethnic origin, to equality before the law, notably in the enjoyment of the […] political rights, in particular, the right to participate in elections-to vote and to stand for election on the basis of universal and equal suffrage, to take part in the Government as well as in the conduct of public affairs at any level and to have equal access to public service."
- The OSCE election-related commitments can be summarized in six key principles noted below that equally apply to assessing legal frameworks for internet voting.[4] The right to an effective remedy and the right to personal data protection (paragraphs 5.10 and 26 of the OSCE 1990 Copenhagen Document, respectively) are also of fundamental importance in the context of elections, including those that include any type of electronic voting. Furthermore, public confidence is an essential element of a democratic election process and has been affirmed in various OSCE documents, including the 2003 Maastricht Ministerial Council Decision No. 5/03.[5]

13. The key principles applicable to developing legal frameworks for internet voting are:

- *Secrecy of the vote*: Paragraph 7.4 of the 1990 OSCE Copenhagen Document requires participating States to "ensure that votes are cast by secret ballot or by equivalent free voting procedure."

- *Integrity of results*: Paragraph 7.4 of the 1990 OSCE Copenhagen Document requires participating States to ensure that the votes cast "are counted and reported honestly with the official results made public".

- *Equality of the vote*: Paragraph 7.3 of the 1990 OSCE Copenhagen Document says that participating States will provide "equal suffrage to adult citizens".

- *Universality of the vote*: Universal suffrage, enshrined in paragraph 7.3 of the 1990 OSCE Copenhagen Document, means that all eligible adult citizens must have this opportunity to participate in elections, and effective means for their participation should be provided.

---

3 See the 2017 CoE CM Recommendation CM/Rec(2017)5 on e-voting and the 2022 CoE CM Guidelines CM(2022)10-final on the use of ICT in elections.

4 These are echoed in the recently published ODIHR Handbook for the Observation of Information and Communication Technologies (ICT) in Elections (2024).

5 See page 61, Decision on elections (MC.DEC/5/03), Eleventh Meeting of the Ministerial Council, 1 and 2 December 2003.

- *Transparency*: Transparency is a cornerstone of OSCE election-related commitments, as it is necessary to verify that elections take place in accordance with the law and democratic principles.

- *Accountability*: The 2003 Maastricht Ministerial Council Decision No. 5/03 underlined the importance of accountability in the electoral process. In the context of internet-based elections, accountability includes election officials, vendors, certification, verification bodies and others involved in the procurement, management and utilization.

14. At the global level, the United Nations has developed guiding principles for business and human rights organizations, including private technology companies, on issues of human rights and political processes.[6] These efforts are supplemented by a number of initiatives led by international organizations focused on advancing democratic electoral processes.[7]

15. To date, no specialised commitments regarding the use of new voting technologies have been developed by the OSCE participating States. However, over the last decades, there has been a concerted effort within some regional international organizations, most notably the CoE, to develop standards and principles that provide further guidelines to its member States. In 2017, the CoE adopted Recommendation CM/Rec(2017)5, setting out standards for electronic voting. This comprehensive instrument includes recommendations, an explanatory memorandum, and supporting guidelines. The 49 e-voting standards are organized under key electoral principles: universal suffrage, equal suffrage, free suffrage, secret suffrage, regulatory and organizational requirements, transparency and observation, accountability, and the reliability and security of the system.[8]

16. The European Union, through its Agency for Cybersecurity (ENISA), has elaborated standards on the security of critical infrastructure for the benefit of EU Member States, EU institutions, and other stakeholders in preventing and responding to cybersecurity threats. Under the EU institutional framework, however, there are currently no specific standards developed on internet voting or other types of electronic voting.[9]

---

6 See the 2019 Report of the UN Secretary-General on Strengthening the Role of the United Nations in enhancing the effectiveness of the principle of periodic and genuine elections and the promotion of democratization in which it states that the United Nations does not encourage or discourage Member States from introducing digital innovations in their electoral operations. While noting their great potential for increasing participation, reducing certain irregularities and strengthening public trust, the report cautions Member States "to take ample time to consider the technical, financial and political feasibility of the innovation through a broad consultative process and of gradually introducing new technology to allow for thorough testing and adjustment, taking into account increasing concerns regarding the vulnerability of national electoral infrastructures to cyberattacks", paragraph 28.

7 Recent examples include Venice Commission, Interpretative declaration of the Code of good practice in electoral matters as concerns digital technologies and artificial intelligence, CDL-AD(2024)044; IFES, Primer: Cybersecurity and Elections, July 2022; General principles and guidelines related to ICT and elections - A Declaration of Principles (DoP) technical document endorsed by the DoP Implementation Meeting, 8 December, 2022; IDEA, Cybersecurity in Elections – Models of Interagency Collaboration, 2019.

8 Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting is a revised and updated version of the CoE's 2004 Recommendation Rec(2004)11. It reflects advances in technology, electoral practice, and experience gained since the earlier text, replacing it with a more comprehensive and detailed framework.

9 See Regulation (EC) No 460/2004 and the EU Cybersecurity Act (Regulation (EU) 2019/881).

17. According to the CoE standards, Member States that introduce e-voting should do so in a "gradual and progressive manner".[10] Member States should develop technical, evaluation and certification requirements and shall ascertain that requirements fully reflect the relevant legal and democratic principles. Member States should keep the requirements up to date. Before an e-voting system is introduced and at appropriate intervals thereafter, an independent and competent body should evaluate the compliance of the e-voting system and of any information and communication technology (ICT) components with the technical requirements, particularly after any significant changes are made to the system. This may take the form of formal certification or other appropriate control. The certificate, or any other appropriate document issued, should "clearly identify the subject of evaluation and shall include safeguards to prevent its being secretly or inadvertently modified." The e-voting system should be auditable, with the audit system open, comprehensive, and actively reporting on potential issues and threats.[11] Furthermore, an electronic voting system requires formalised procedures to monitor its security and reliability and rectify any problems (Guidelines(2017)5, on Standard no. 40).[12]

18. Furthermore, CoE standards require that the relevant legislation regulates the responsibilities for the functioning of e-voting systems and ensures that the electoral management body (EMB) has control over them (Standard 29). The responsibility for compliance with all requirements should be with the EMB, including in the case of failures and attacks. The EMB should remain responsible for the availability, reliability, usability and security of the e-voting system (Standards 29 and 40). There are numerous stakeholders that play a role and bear some degree of responsibility in developing, testing, deploying, applying, maintaining, observing, and auditing e-voting systems. Ultimately, however, it is the EMB that bears the overall responsibility for the voting processes and, thus, for the e-voting system. The relevant legislation should provide for the supervisory role of the EMB over e-voting. The role and responsibilities of the other parties involved should be clarified at the appropriate regulatory or contractual level (Explanatory Memorandum, paragraph 87 on Standard 29).

19. CoE standards also address transparency and observation of the e-voting process, calling on Member States to be transparent in all aspects of e-voting (Standards 31 to 35, Rec(2017)5).[13] This includes the timely publication of comprehensive information on all software and hardware components used, including their versions, configurations, and certification results, as well as public access to documentation, source code, and audit protocols disclosed well in advance of elections to allow meaningful scrutiny by stakeholders.

20. The ODIHR Handbook for the Observation of ICT in Elections provides detailed guidance on observing internet voting as part of a broader framework for assessing New Voting Technologies (NVT) and ICT in electoral processes.[14] It identifies internet voting as the least used but among the most discussed forms of NVT. The handbook underscores the importance of individual and universal verifiability in internet voting systems and notes that such systems often rely on cryptographic solutions and trust in system operators. The handbook recognizes

---

10 Standard 27, CoE's Recommendation of the Committee of Ministers to member States on standards for e-voting Rec(2017)5.

11 Standards 36, 37, 38, 39, Rec(2017)5.

12 Guideline on Standard 40, Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting, of 14 June 2017, CM(2017)50-add2final.

13 See also Guideline 7 of the CoE Committee of Ministers' Guidelines on the use of information and communication technology (ICT) in electoral processes in CoE member States, CM/2022/10.

14 See ODIHR Handbook for the Observation of ICT in Elections.

the existence of procedural safeguards that may mitigate risks, but also stresses that internet voting requires rigorous cybersecurity measures, clear legal frameworks, transparency, and public confidence to be considered in line with OSCE commitments.

3.2. Background

21. Internet voting has been used in Estonian elections for the past 20 years, starting with the 2005 local elections. Upon invitation from the Estonian government, ODIHR has observed all five *Riigikogu* elections in which internet voting has been used (2007, 2011, 2015, 2019, 2023). Internet voting has been further used during local elections (2005, 2009, 2013, 2017, 2021) and European Parliament elections (2009, 2014, 2019, 2024).

22. ODIHR's Final Report on the 2023 parliamentary elections concluded that "[t]he legal framework constitutes a sound basis for the conduct of democratic elections, in line with international standards", which included amendments that addressed some previous ODIHR recommendations related to internet voting. Noting that e-voting enjoys a relatively high level of public trust in Estonia, ODIHR found that "[t]he internet voting process was organized professionally and transparently, with due attention to accuracy and security of the underlying systems, but with some technical difficulties". It noted that e-voting "faced claims of electoral fraud by some political actors that remain unsubstantiated, which had a detrimental impact on the trust among a considerable number of voters and led to polarisation along political party lines in the choice of voting method."

23. ODIHR has put forward various recommendations aimed at further enhancing the legal framework for internet voting and its implementation in line with international standards and good practice. These recommendations are generally related to developing technical specifications, enhancing security and risk mitigation, and ensuring accountability and transparency, all aimed at strengthening the transparency and reliability of e-voting and public trust in the electoral process and results. In the last 10 years (since the 2015 parliamentary elections), ODIHR has issued a total of 18 recommendations related to internet voting. While ODIHR has not yet formally evaluated the seven recommendations on internet voting it made related to the 2023 parliamentary elections, and this will be formally conducted by the potential ODIHR election observation or assessment mission during the 2027 parliamentary elections, some recommendations were fully or partially implemented, and some remain to be addressed.[15]

24. Among the recommendations addressed are that the Electronic Voting Committee (EVC) now meets regularly and formally publishes all decisions related to internet voting in sessions open to observers.[16] The EVC has also reviewed its security practices related to server maintenance and backup and now produces and retains records at many stages of the process, as per other recommendations made. The Estonian authorities have also mostly met previous recommendations on making efforts to ensure individual and universal verifiability in their

---

15 For the full overview of these recommendations, please see ODIHR's dedicated repository of recommendations it has issued, together with the implementation status.

16 This is notwithstanding the recent Supreme Court decision 5-25-3 of 11 April 2025, which found that the partial limitation placed on an observer's remote attendance was in accordance with the Constitution and the law.

internet voting system so as to enhance accountability through verification. This is line with the ODIHR ICT Handbook, specifically paragraphs 2.1.1 and 2.1.2.[17]

25. ODIHR is aware that, despite existing international good practices and recommendations for regulating internet voting, no country has implemented all recommendations, such as those put forward by the CoE. However, no other OSCE participating State has successfully introduced internet voting for all voters and in all constituencies, and no other country has the level of public trust in internet voting that has resulted in it becoming the main voting channel, as in Estonia during the 2023 Parliamentary elections.

26. Estonia is the only country to have provided internet voting to all eligible voters and has continued to do so since 2005. Internet voting is used in addition to voting at polling stations on election day, advance voting in polling stations, home voting limited to persons unable to go to the polling station, postal voting limited to Estonians living abroad who can mail their vote to an Estonian diplomatic mission abroad, and voting in-person at diplomatic missions, penal institutions, hospitals, and 24-hour social welfare institutions. As per ODIHR's ICT Handbook, internet voting can thus positively enfranchise a greater proportion of citizens living abroad as well as homebound voters and those who face difficulties going to polling stations in person.[18] Voters can cast their ballots online during the advance voting period, which starts on Monday at 9 a.m., six days before the Sunday election day, and runs uninterruptedly until Saturday, a day before election day, at 8 p.m. A few other countries in the OSCE region use internet voting, however, in a limited way, on an experimental basis, such as a digitized form of postal voting.[19]

27. The percentage of voters using internet voting in Estonia has increased over the years, with a record 51.1 per cent of i-voters among participating voters at the 2023 parliamentary elections (overall turnout was 63.5 per cent of all registered voters). In this election, internet voting became the most used voting channel for the first time. In the 2024 European Parliament election, the percentage of internet voters was lower, at 41.7 per cent (overall turnout was 37.6 per cent).[20] According to research, internet voting in Estonia has not increased overall participation but may have prevented a decline in participation.[21]At the same time, Estonia has seen a certain degree of reduction of trust in e-voting among voters, largely due to the challenges and questions about its integrity raised by some political parties. Claims in this regard for the 2024 elections were found to be unsubstantiated. This has also led to a polarisation of public

---

17 The implementation of comprehensive universal verification methods by the authorities means that "all votes must be cast in a ballot box as the voters marked them; all votes must be counted as cast; and no votes should be illegally added to or subtracted from the results. There must be no possibility for fraud or error to alter the results." ODIHR Handbook for the Observation of Information and Communication Technologies (ICT) in Elections (2024), paragraph 2.1.2. See also paragraph 2.1.1.

18 "Internet voting has the potential to provide easier access and more options for participation in elections, especially for voters facing barriers to accessing polling stations or those living outside their official residence area." ODIHR Handbook for the Observation of Information and Communication Technologies (ICT) in Elections (2024), paragraph 2.1.4.

19 For the 2023 Federal Assembly elections, the Swiss federal government authorized internet voting trials for a maximum of 10 per cent of the federal electorate to use the current internet voting system. French voters residing abroad can vote via the internet to elect their representatives in parliament. Some jurisdictions in the United States provide a possibility for casting ballots remotely, over the internet.

20 See internet voting statistics in Estonia.

21 Ehin et al., Internet voting in Estonia 2005–2019: Evidence from eleven elections - ScienceDirect

opinion.[22] At the same time, some political parties have introduced proposals for more ICT in future elections.

28. Political parties with parliamentary representation, whose members expressed concern over the current use of internet voting during meetings with ODIHR experts, included representatives of the Conservative People's Party of Estonia (EKRE), the Centre Party, and *Isamaa* (Fatherland). EKRE has been historically opposed to internet voting. They currently have four main areas of concern: end-to-end verifiability (E2EV), protection against internal threats (insider attacks), the system for independent auditing and observation, and the system for filing complaints. Their position is that until E2EV can be implemented in a manner to their satisfaction, the use of internet voting in parliamentary and European Parliament elections should be suspended. They envisage reintroducing it once it has been proven, at a lower level than the general elections, to be capable of offering guarantees equivalent to voting with paper ballots and pending a constitutional review of the applicable legal framework.

29. The Centre Party holds a similar position to EKRE, but instead of aiming to abolish internet voting, it seeks to improve its security. *Isamaa* members criticized the current verifiability of internet voting, uniformity between in-person voting legal requirements and those applying to internet voting, the delegation of power to decide on mobile voting given by parliament to the NEC, as well as the current level of control of the state over choices made by private companies involved in internet voting. *Isamaa* representatives were also concerned about coercion, especially in care homes and about the persistent rumours of abuses and lack of prosecution of such cases. They claimed that coercion had become more sophisticated and widespread during local elections.

30. Both the Centre Party and *Isamaa* proposed the introduction of a face recognition system to avoid impersonation, especially of people living in care homes. The representatives of all three parties stated that the use of internet voting is not politically neutral despite it being equally available and accessible to all voters. They reasoned that the ruling majority won the internet vote, whereas the opposition won the in-person paper vote in 2023.

31. Parliamentary political parties that fully support the current use of internet voting include the Reform Party, the Social Democratic Party and Estonia 200. Their trust is reportedly based on trust in the institutions in charge of internet voting, namely the NEC and SEO, their explanations to the parliament about identifying and fixing problems or breaches, trust in the qualified auditor and the positive results noted in the 2022 audit report, the fact that different processes including counting of electronic votes are public and that coercion and lack of secrecy can be countered by re-casting the vote (either electronically or in-person). This is in line with the ODIHR Handbook on ICT.[23] Other factors that contribute to their confidence are Estonia's

---

22 A public opinion survey related to electronic voting in Estonia was commissioned by EKRE and carried out by Norstat, a specialist survey firm, on 23 April 2023, following the parliamentary elections. According to its result, 38% of respondents did not consider e-voting in Estonia to be reliable, and 39.7% of the respondents believed that the elections could have been partly tampered with. To the contrary according to a study by a group of experts, in previous years, the public trust in e-voting in Estonia was as high as 70-80% (see Chapter 5.3 of the following study).

23 This states that "when NVT systems give voters receipts or codes to verify that the vote was recorded as cast, supplementary measures should be implemented to safeguard the secrecy of the vote in accordance with OSCE commitments.", ODIHR Handbook for the Observation of Information and Communication Technologies (ICT) in Elections (2024), paragraph 2.1.1.

unique approach to the use of electronic IDs (e-IDs) and the fact that other online transactions, such as e-banking, are not questioned at any level (in terms of privacy, accuracy, or security). Proponents from these political parties and many other stakeholders, including from the expert community, believe that distrust is politically motivated rather than an issue related to the quality of the law or technical questions. They also noted that those in the opposition had the opportunity to thoroughly investigate the issue of internet voting in particular in the period in which they were participating in government coalitions.[24] They furthermore noted that any alleged violation should be reported to the public prosecution.

32. Internet voting in Estonia is conducted by voting from a personal computer. Voters can also use a separate verification channel with a smartphone. As of 1 October 2024, the law has enabled the NEC to decide whether to permit voting from mobile devices. The NEC has not yet authorised voting through mobile devices due to certain technical and conceptual obstacles but it is looking into possible solutions.[25] Another development relates to voter identification. In addition to the state-issued e-ID (for which a card reader is required) or a state-issued mobile ID (for which a SIM card is required), the REA now allows identification through other documents that meet the digital identification requirements provided in provided in the Identity Documents Act.[26] This new rule was introduced to facilitate the use of the Smart-ID system, which is application-based (not requiring specialized hardware such as a card reader) and is the most widely used system in Estonia for all types of electronic identification services.[27] ODIHR interlocutors commented on these developments, but the legal adaptations that they entail are outside the scope of this Opinion.

3.3. Legislation related to Internet Voting

33. In its Opinions on electoral legislation, ODIHR and the CoE's Venice Commission have consistently expressed the view that any successful changes to election laws should be built on at least the following three essential elements: 1) clear and comprehensive legislation that meets international obligations and standards and addresses prior recommendations; 2) the adoption of legislation by broad consensus after extensive public consultations with all relevant stakeholders; and 3) the political commitment to fully implement such legislation in good faith, with adequate procedural and judicial safeguards and means by which to evaluate shortcomings in a timely manner. Further, fundamental elements of electoral law should not be open to

---

24 From November 2016 until April 2019, the Centre Party was in the ruling coalition with SDE Pro Patria and Res Publica Union, which was later renamed *Isamaa*. From April 2019 until January 2021, the ruling coalition included EKRE, Centre Party and *Isamaa*.

25 The ODIHR expert team was informed that the biggest technical obstacles to introducing voting via mobile devices are how to provide for a separate vote verification channel if the voter has one mobile device and how to retain full control over the application distribution, which currently has to be shared with the application store providers.

26 The NEC establishes the electronic identification procedures used for the identification of voters (§48^2(3)1 REA). In addition to the state-issued e-ID (§48^5(2) REA), equivalent electronic identification means may be used (§48^5(2) REA).

27 To get a Smart-ID issued, citizens must identify either through an existing state-issued e-ID or mobile ID or through biometric identification provided by certain certified banks that also require the provision of a valid passport or ID card.

amendment less than one year before an election.[28] In general, any reform of electoral legislation to be applied during an election should occur early enough for it to be effectively implemented for the election.[29]

34. In Estonia, internet voting followed the introduction of other relevant acts, namely, the Identity Documents Acts (1999), which includes detailed provisions for digital identity cards, including digital identification via mobile ID and the Digital Signatures Act (2000), which regulates the use of legally binding digital signatures, along with the provision of certification and time-stamping services. Subsequently, other related legislation was adopted, the Population Register Act (2017) and the Personal Data Protection Act (2018), which regulate the use of data recorded in the Population Register, the state's primary database containing information on all Estonian citizens and residents.[30] Internet voting is regulated by four electoral laws: the *Riigikogu* Election Act (REA), the Local Government Council Election Act, the European Parliament Election Act and the Referendum Act. However, the main regulation of internet voting is found in the REA, while other electoral laws refer to the REA, a legislative approach that positively ensures coherence by providing that the rules for internet voting are the same for every election. When changes occur in how elections are conducted, all four laws are amended simultaneously, which is a constructive approach.

35. The REA was introduced in 2002. It includes provisions which apply to all voting channels: general provisions (§1 ff), provisions on electoral management (§9 ff) and election managers (§13 ff; including §18^1 on the election information system, electronic voting system and ensuring cybersecurity as well as §19^4 on observation), provisions on registration of voters (§20 ff), on voting procedures (§34 ff), on voting from abroad (§49 ff), on ascertaining of voting results (§57 ff), on election expenditure (§64), on notices and complaints (§68 ff), on liability (§73^1 ff) and final provisions (§74 ff). The REA includes further provisions that apply exclusively to internet voting; these are mainly Articles 482 to 4812 (Chapter 71 on electronic voting) as well as a few other articles scattered throughout the REA. REA e-voting provisions were last updated on 24 May 2024.[31]

36. Modified and new provisions introduced in 2024 address the competences of the SEO (§15(2)5^3, §18^1) and of the Information System Authority (RIA) (§18^1), the general principles of electronic voting (§48^2), the preparation of e-voting (§48^3), the organisation of the e-voting system (§48^4), the electronic voting procedure (§48^5), secrecy (§48^6), security (§48^7) and integrity (§48^8), the change of e-votes (§48^9), verification of e-votes (§48^{10}), the taking into account of e-votes (§48^{11}), the suspension, termination and not starting of e-voting (§48^{12}),

---

28 Venice Commission Code of Practice in Electoral Matters, Guideline II.2.b. According to the Venice Commission's 2005 Interpretative Declaration on Stability of the Electoral Law (CDL-AD(2005)043), fundamental elements include the electoral system proper, rules relating to membership of electoral commissions, and rules on the drawing of constituency boundaries. Further, the principle according to which the fundamental elements should not be amended less than one year prior to an election does not take precedence over the other principles of the Code of Good Practice in Electoral Matters and should not be invoked to maintain a situation contrary to the norms of European electoral heritage or to prevent the implementation of recommendations by international organizations.

29 Part II, paragraph 5 of the Venice Commission 2005 Interpretative Declaration on Stability of the electoral law (CDL-AD(2005)043).

30 For an overview of internet voting development in Estonia, see Ehin et al., Internet voting in Estonia 2005–2019: Evidence from eleven elections (2022).

31 REA modifications were adopted by the Riigikogu on 24 May 2024 and entered into force partially on 3 June 2024 and partially on 1 October 2024.

verification of integrity of e-votes and verification of integrity of e-voting system's data during the counting of e-votes (§60[1](1[1]) and (9[1])), destruction of back-up copies of the system and personal data therein by other parties involved in the organisation of e-voting (§77[1](2)2) as well as expenditure, namely for the RIA (§65(6)). Most of the 2024 changes in the REA are provisions transposed, in many cases *ad verbum,* from the NEC regulation and represent a positive effort to ensure these issues are regulated in primary legislation.[32]

37. The novelty, therefore, consisted in transferring them from the lower-level regulations to the primary law, as approved by the parliament, which increased the legal certainty. The amendments address several provisions outlined in the CoE Recommendations, including the publication of technical requirements for e-voting, the provision of greater detail in auditing the system, and the specification of greater detail on various e-system components, their verification, integrity, and handling of personal data.[33] This is also in line with the criteria set out in the ODIHR ICT Handbook.[34] Completely new provisions introduced in 2024 include two possible future developments whose actual deployment *may* be decided by the NEC. These include extending internet voting to mobile devices and allowing the use of an alternative electronic system for voter e-identification.[35]

38. The decision to modify the REA was part of the Programme of Government and intended to bring the legislation in compliance with the judgements by the Supreme Court in 2019 and 2023, which called for internet voting to be further regulated at the legislative level.[36] The draft was prepared by the Ministry of Justice and Digital Affairs (MJD) in July 2023, followed by internal consultations with other ministries and consultations with stakeholders, including the NEC, SEO, all political parties, local government, and Tartu University. According to the available documentation, the MoJ list of those consulted does not include any civil society.

39. Three stakeholders, including one political party (*Isamaa*), submitted opinions at this stage. The draft amendments were published, and the public had the opportunity to provide opinions and suggestions. Some proposals including the NEC proposals were taken into consideration, and the draft was revised by the MJD, after which a second round of internal consultations was held. The draft was then discussed in Parliament by the Constitutional Affairs Committee, which held six hearings organised over two to three months, at which some experts or interested groups

---

32 Following the adoption of the amendments, the NEC regulation "Technical requirements to ensure the general principles of organizing electronic voting" and "Description of the electronic voting organization" (both from 9 February 2024) ceased to exist. The currently standing NEC regulations include "Establishment of the form of the ballot and electronic vote" (20 September 2023) and "Establishment of electronic identification systems used for voter identification" (9 January 2025).

33 CoE Recommendations CM/Rec(2017)5 and CM(2022)10.

34 See ODIHR Handbook for the Observation of Information and Communication Technologies (ICT) in Elections (2024), table 5.

35 In January 2025, the NEC issued a decision allowing voters to identify themselves through the Smart-ID system.

36 A 2023 Supreme Court judgement held that, in line with the specified constitutional norm the legislature was obliged "to provide for sufficiently tight regulation in the electoral laws on all important issues concerning elections, in order to ensure the legislature's control and public trust in the elections through organization, procedural and substantive legal guarantees."

that had comments or suggestions on the bill were invited to be heard.[37] Two parties provided responses; the opposition made several proposals, including to suspend e-voting; however, no consensual agreement could be found. The amendments were approved by the ruling majority without opposition support.[38]

40. Provisions implementing electoral principles, such as universal, secret, and secure elections, were introduced to the REA in 2024, detailing requirements that apply to internet voting. In another advancement, provisions for cybersecurity were introduced, which had not been previously included.[39] This is in line with guideline 4 of the CoE Recommendation CM(2022)10 and with provisions in the ODIHR ICT Handbook.[40] These represent an important modification of the REA to the extent that such provisions contain interpretations of the principles that differ from the interpretation given in the context of paper voting and introduce a level of stability that was not offered by the lower-level regulations. However, when asked about past discussions in parliament, since the beginning of internet voting, on the concretisation of constitutional principles in legal norms that regulate internet voting (REA and lower-level acts), MPs informed ODIHR that a detailed discussion on how to adhere to constitutional principles in regulating internet voting has not taken place in the parliament or public. One main reason appears to be the difficulty for the public, including members of parliament and professionals in the legal and IT fields, except for a few specialists, to grasp all the technical intricacies of internet voting. This observation applies equally to other participating States. Ultimately, it is up to the parliament and the public to decide, based on an informed discussion and broad political backing, whether to place their trust in the experts—namely, the NEC, the SEO, the RIA, and the specialists they appoint or engage.

41. According to the information received by the ODIHR expert team, a comprehensive discussion of the interpretation of electoral principles in the context of internet voting has not taken place, including at the time when the NEC and SEO regulations were first introduced. **It is therefore recommended that any substantial modifications are introduced only following broad consultations within the parliament and with the public to strengthen the law's legitimacy and public acceptance.**

42. **Furthermore, given the technical complexity of internet voting, it is essential that a group of experts, including academics and civil society experts, address critical arguments constructively and transparently. Presenting the arguments in language that the public can understand is necessary. Important changes to the REA, such as introducing or modifying internet voting, should receive broad backing from political forces in Parliament.**

---

37 Shortly after the Committee had finished preparing the second reading of the bill, the NGO Fair Elections sent a letter to the Committee requesting the inclusion of collective court petitioners who had previously expressed critical views on e-voting legislation. In its reply, the Committee stated that it was aware of these proposals, as they were set out in their collective appeal, which the Committee had already discussed and rejected with the relevant justifications beforehand.

38 The details and results of the consultation process, as published in the Official Gazette, can be found here.

39 This is in line with ODIHR's 2024 Handbook for the Observation of Information and Communication Technologies (ICT) in Elections, which notes the importance of this issue to ICT and e-voting integrity.

40 See CoE Recommendations CM(2022)10, guideline 4 and ODIHR Handbook for the Observation of Information and Communication Technologies (ICT) in Elections (2024), Chapter 7.

RECOMMENDATION A.

To introduce any future substantial modifications to the legal framework governing internet voting only following broad-based consultations and demonstrable support within Parliament and among the public in order to enhance the legitimacy of the law and further strengthen public confidence. Given the technical complexity of internet voting, such discussions should meaningfully involve a representative group of experts, including academia and civil society experts.

43. Chapter 7^1 of the REA includes provisions on the interpretation of electoral principles, requirements on organisation, technical implementation and controls. These are elaborated in 11 articles organised around the interpretation of general principles (§48^2), the organisation of the different phases of the vote (§§ 48^3-48^5), ensuring higher principles (§§48^6-48^{11}), including secrecy, security, and integrity, and the options of suspension, termination or not initiating internet voting (§48^{12}).

44. The 2024 REA amendments have clearly improved the readability of the regulation by consolidating provisions that were previously included in lower-level regulations. Still, some further improvements appear necessary to ensure that the law explicitly and systematically addresses legal, technical, control and organisational requirements that apply to internet voting, thereby enhancing respect for electoral principles in internet voting. **It is therefore recommended that legislators further develop the legal requirements aimed at implementing the electoral principles of universality, equality, secrecy, and the free exercise of voting rights. The main legal requirements that apply, among others, to the system's and/or the information's (including personal data) accessibility, usability, availability, reliability, confidentiality, integrity, authenticity, verifiability, underlying trust assumptions, transparency, observability, cooperation with third parties, risk management, controls, responsibilities, dispute resolution, should be explicitly introduced or further clarified and developed.**

RECOMMENDATION B.

To further develop the legal requirements aimed at explicitly providing for the implementation of the electoral principles of universality, equality, secrecy, and free exercise of voting rights in the context of internet voting.

45. On the principle of vote secrecy, from a point-of-voting perspective, this can be respected when using a remote voting method, provided that the law guarantees the right to vote in secret and has certain safeguards. These include sanctions for any violations. However, it should be noted that all voting methods are to some extent susceptible to breaches of vote secrecy and may be open to pressure, coercion, intimidation or exposure to illegal incentives. Secrecy, therefore, depends on procedural safeguards, conditions at the time of voting, political culture and implementation of dissuasive measures to prevent electoral malfeasance.

46. For this reason, voting channels outside controlled environments, including postal or internet voting, are considered more vulnerable. In Estonia, voting in secret is a constitutional right. Under the REA, the challenge to respecting this right is addressed by allowing voters to change or override their vote online, either by electronic means as many times as they wish or by submitting a paper vote in advance or on election day. This measure is designed to address potential violations of secrecy or the right to vote freely**. To further strengthen the right to**

cast an e-vote freely and in secret, additional measures can be instituted. These can include providing ongoing voter education to explain these electoral principles and applicable sanctions. Instructing voters immediately before casting the vote that it must be done in secret and requiring them to confirm (declare) that the vote is being cast without coercion and/or that sanctions apply in case of violations by third parties trying to manipulate or pressure voters are established. Such a declaration might simply involve checking a box or pressing a button to confirm agreement, serving as a straightforward additional step in the voting process.

RECOMMENDATION C.

To further strengthen the existing safeguards of the right to cast an internet vote freely and in secret, additional measures could include continuous voter education on these principles, clear instructions at the time of voting emphasizing the requirement to vote in private, and the introduction of a mandatory declaration confirming that the vote is cast in secret and without coercion.

47. The principle of secrecy of the vote can be susceptible to abuse in the context of voting in group settings, such as care homes, or where the same computer (or smartphone) is provided by third parties for multiple voters to cast internet votes. Given that such abuses have been alleged in previous Estonian elections, it is advisable to provide special attention to address these risks. **In this respect, it is recommended that the NEC and SEO be legally obliged to monitor for such infractions on the system side, which can be partially automated with RIA's assistance, in other words, to formalize in the law the monitoring practice using digital tools that is already conducted informally, and also to conduct post-election audits in these settings, with field visits if needed, to determine if any such breaches or attempted breaches have occurred. Furthermore, identified perpetrators should be prosecuted, with dissuasive and proportionate sanctions imposed (see also paragraph 71).**

RECOMMENDATION D.

To legally oblige the National Election Committee (NEC) and State Election Office (SEO), assisted by the Information System Authority (RIA), to monitor potential breaches of the voting system and to introduce explicit requirement for post-election audits to determine if any breaches have occurred, specifically those related to secrecy of the vote in cases where group voting or voting in a sequence using the same device may be suspected.

48. At the organisational level, the main institutions involved in organizing internet voting are the NEC, SEO and RIA. As called for by international standards for electronic voting, the NEC is an independent agency whose main task is legal supervision of all decisions and steps taken in connection with elections.[41] The NEC supervises the conformity of internet voting with the main principles of elections, which are legally prescribed. The REA gives the NEC the power to decide on the use of internet voting, to certify its results, to sanction violations, and to hold a repeat internet vote. The NEC should ensure that the general electoral principles outlined in §1(2) and (3) of the REA are upheld, including in e-voting. The NEC ascertains the results (§ 61), supervises election managers, namely the SEO, resolves complaints (§§ 69, 71, 72, with

[41] See further information about the NEC.

the last instance being the Supreme Court, § 721), and performs other functions arising from the law (§ 9(1) REA).

49. Also in line with ODIHR guidance, the NEC declares the electronic voting results invalid in whole or in part and orders a repeat vote where a violation significantly affected or could have significantly affected the voting results (§9(2)3, see also §73). It decides not to start electronic voting or to suspend or terminate it in whole or in part where the security or reliability of the electronic voting system cannot be ensured in line with the requirements of REA and notifies the voters (§9(2)4 and 1, §48^{12}(1)). The NEC not only has the right but also the obligation to take any of the decisions mentioned as soon as certain conditions of §9(2) 3 or 4 REA materialize (§9 (2) and (1)).[42] In addition, the NEC has regulatory power to introduce detailed technical provisions on internet voting. In particular, it establishes the standard form of electronic votes (§37(1));[43] it establishes the electronic identification schemes used for the identification of voters and decides on the use of smart IDs in addition to the state e-ID (§48^{2}(3)1); establishes the technical requirements for electronic voting (§48^{2}(3)2); determines the operating systems for which the voter application and the vote verification application are created and thus decides on the potential future use of mobile voting (§48^{3}(5)).

50. Furthermore, the NEC participates in the operations by receiving shares of the vote-opening key (§48^{3}(3)) and participating in the counting of electronic votes (§60^{1}(2), (4)). In accordance with international good practice for Election Management Bodies, the NEC decides on issues within its competence by a majority vote, and all members (or their substitutes) have to be present (§12(5), (7) REA).[44] Further, members of the NEC must be impartial and independent in the performance of their duties (§11(4) REA). As a positive transparency measure, meetings of the NEC are public and recorded in minutes (§12(3) REA).[45] Complaints against the NEC's resolutions and acts can be lodged with the Supreme Court (§§69, 71).

51. In summary, the provisions of the REA enable the NEC to make decisions regarding the initiation or non-initiation of electronic voting, as well as the suspension or termination of this process, depending on whether the specified conditions are met or not. Additionally, the NEC is mandated to decide to invalidate internet voting results if there is a violation of the conditions and if the violation significantly affected or could have significantly affected the voting results

---

42 The condition to decide not to start, or to suspend/terminate e-voting is where the security or reliability of the e-voting system cannot be ensured in such a way that e-voting could be conducted pursuant to the requirements of the REA (§9(2) 4) and the condition for declaring the e-voting results invalid and holding a repeat electronic vote are the identification of a violation that significantly affected or could have significantly affected the voting results (§9(2) 3). The REA also foresaw that the verification of electronic votes as provided for in §48^{6} – a change in the system – could not be implemented before a certain year, but that the NEC *could decide on the experimental use* of the verification system offering individual verifiability during earlier local elections (§85^{1} REA).

43 See also NEC decision No. 92, adopted 20.09.2023

44 The NEC comprises seven members appointed respectively by the Chief Justice of the Supreme Court (two members), the Chancellor of Justice, the Auditor General, the Chief Public Prosecutor, the State Secretary and the Estonian Auditors' Association (each one member) for a four-year term (§10(1) 1 to 7 REA).

45 In this regard, there was a recent Supreme Court ruling, dated 5-25-3 of 11 April 2025, regarding the level of openness required of the NEC for those participating remotely. The Supreme Court ruled that it is within the NEC's legal jurisdiction to limit access to those not attending in person. In its ruling, however, it noted that "…the Supreme Court has not yet developed a unified position on the form of observer participation in such an election committee meeting that takes place both electronically and on-site", and there is a dissenting opinion in this regard.

(§9(2)4 REA). The main condition is the upholding of the main electoral principles (§1(2), (3) and §9(1) REA). Other conditions should be found in the detailed legal requirements of §48[2] and the following articles.

52. It is not clear in the legislation, however, which criteria the NEC would use to decide whether not to start, suspend or terminate internet voting. Furthermore, the NEC oversees the SEO, which conducts internet voting, resolves complaints against election managers, participates in internet vote counting, and holds part of the cryptographic key for opening the ballots. **To ensure legal clarity and prevent potential arbitrary decision-making, it is recommended that the legislator establishes clear and objective criteria in the REA, based on which the NEC would decide not to start, suspend, or terminate electronic voting, or declare its results invalid. Further, it is recommended to legislate clear conditions based on which the NEC can decide to implement or discontinue the use of mobile devices for internet voting.**

> **RECOMMENDATION E.**
>
> **To establish clear and objective criteria for decisions by the NEC in the election law not to initiate, suspend, or terminate electronic voting or to declare its results invalid. Furthermore, it is recommended that clear conditions are legislated under which the NEC may decide to introduce or discontinue the use of mobile devices for internet voting.**

53. The SEO, a structural unit of the *Riigikogu* Chancellery, is independent in performing its duties under the REA. They are overseen by the NEC (§13(1)1 and §14(1), (5)). For internet voting, the SEO is responsible for the following important safeguards of the process:

- ensures the legality of elections, organises internet voting, and determines its results. It also develops, operates, and maintains the election information system and electronic voting system, including the online voter register and tools for encrypting, decrypting, processing, and counting e-votes. It ensures that the system remains up to date and that each vote is correctly counted or annulled and reflected in the results;
- configures all system components before voting, approves the security policy and NEC guidelines, and determines the cryptographic algorithm. It sets up and shares encryption and decryption keys. It also develops the verification application and publishes the source code for the voting and verification systems (not the voter application);
- develops, administers, hosts, and secures the systems. In this, the SEO may involve competent authorities and private companies (e.g. Cybernetica for software, KPMG for audits). Other contracted services may include timestamping, identification, and registration.
- organises test voting, publishes its schedule and results, and commissions independent audits covering test voting, system integrity, and legal compliance. It allows information requests under the Public Information Act.
- resolves incidents, verifies vote integrity and digital signatures, checks if e-voters are on the voter list, and annuls e-votes overridden by paper votes—retaining only the last valid vote per voter. It ensures the separation of personal data from votes, oversees counting, verifying the results the day after election day, with the head of the SEO signing the final outcome.
- destroys un-anonymised e-votes, logs, and personal data after the election while retaining anonymous logs. It handles notices of deficiency against election managers and transmits complaints to the NEC.

54. The RIA is a state agency responsible for further assisting the internet voting process by providing:
    - technical development, operation, hosting, and cybersecurity of the election information system, and for hosting the collector component (electronic ballot box) of the e-voting system. Additional tasks may be assigned through agreements with the SEO. While cybersecurity of the e-voting system is not explicitly listed as RIA's duty, it may be included by agreement.
    - providing election-related services under a Service Level Agreement (SLA) with the SEO, which defines RIA's responsibilities and the roles of other stakeholders, including the election auditor. The SEO maintains control over the process through a joint task force with RIA representatives. This task force can submit proposals to the NEC during the election period.
    - performing general risk assessments and managing risks in accordance with the Cybersecurity Act. If it identifies risks that cannot be mitigated, it informs the SEO, who holds ultimate responsibility as the designated risk owner. RIA is ISO27001/EITS certified.
    - Transferring all election-related data on a CD to the SEO premises under police escort, with the auditor observing the handover. However, the configuration of servers before the election is not audited. Any citizen's request for election information submitted to RIA is forwarded to the SEO for consideration.

55. The above provisions indicate that the SEO holds operational responsibilities across all aspects of the system—including registers, the voter and vote verification applications, and the counting process—along with necessary control and verification responsibilities over both the vote and the results. Given its limited capacities dedicated to internet voting, the SEO delegates crucial tasks, namely the establishment of software, hosting tasks, and control tasks, to contracted providers, including state agencies (e.g., RIA) and private ones. It does so based on technical, security and organisational requirements, which are reportedly outlined in bilateral agreements but are generally not published.[46]

56. In addition to the established legal principles and certain legal requirements, the REA contains some organisational and technical requirements or references to technical requirements to be introduced by the NEC or the SEO (for instance, the SEO determines the exact specification of the cryptographic algorithm before the election (§48^7(3)). The legal framework, as described above, does not sufficiently elaborate on the safeguards of the internet voting process**.** To address this, **it is recommended that technical, organisational, security and control requirements (hereinafter, technical requirements) that implement the legal requirements specific to internet voting be further clarified and explicitly elaborated.** The REA should explicitly stipulate that the technical requirements must fully comply with the legal requirements and be guided by state-of-the-art technology standards and good practice**.** Although it is a good practice to consolidate technical requirements in one regulation, it may not be appropriate to include them in the REA, as they may need to be frequently updated. Bearing in mind the years of experience and the established and tried-and-tested framework,

---

[46] Parliament maintains an online documents register, where *inter alia* all decisions and other documents pertaining to internet voting are publicly disclosed. The contracts are typically not published, as the law requires the protection of personal data, sensitive information related to the security of the systems, and trade secrets of the contracted companies.

the NEC may be the most appropriate body responsible for introducing and updating the technical requirements, as currently provided by the REA.

57. However, **to ensure respect for all the legal principles involved, the technical requirements should be defined and updated in a consensual and transparent manner and considering the inputs of a representative group of experts, including academia and civil society experts, as required by international good practice, and possibly international observers (given the small size of the community of internet voting experts). To maintain transparency, the most important discussion elements should be published in a language that is easy for the public to understand.**[47] **If, during the defining of the technical requirements, it becomes clear that the technology does not allow or ceases to allow full implementation of the legal requirements established in the REA, the NEC should be required to bring the question to the legislator. It has the authority to reshape internet voting, introduce a different interpretation of principles, or otherwise legislatively address the matter. If the legislator delegates the power to introduce technical requirements that potentially restrict electoral rights to the government or an independent state agency, the legislator should clearly define the scope of these potential restrictions**.

RECOMMENDATION F.

To further clarify and develop the technical, organisational, security, and control requirements that give effect to the legal provisions on internet voting, ensuring they continue to reflect state-of-the-art technology standards and international good practice. These requirements should be defined and regularly updated through a transparent and inclusive process, that incorporates input from a representative group of experts, including academia and civil society experts.

58. **It is further recommended that the legislator clarify all types of control required for the system and its procedures in the REA, including checks to verify that technical requirements, including organisational and security, are correctly implemented. These should include controls that take place before a new system is implemented, controls that occur whenever major changes in the system occur, and periodic controls, as well as their regulation (in terms of who implements them and how). The REA should also specify that controls should be conducted by independent bodies. The detailed regulation of controls should be part of the technical requirements and aim at complying with state-of-the-art technology and good practice.**

RECOMMENDATION G.

To explicitly define in the REA all types of control and oversight mechanisms required for the internet voting system in place and related procedures and to ensure that such controls are carried out by independent bodies. The applicable regulations should aim to reflect state-of-the-art technology and align with international good practice.

---

47 Publications on the discussions can, for example, be similar to the current publication of meeting minutes by the Academy of Science Cybersecurity Committee.

59. **To further enhance transparency and increase public trust in the e-voting process, it is also recommended that the REA clarifies which controls can also be conducted by the interested public (e.g., observers with specialist knowledge, national and international experts) as well as the testing modalities and transparency measures to enable some controls by the public. The detailed regulation, for instance, of the publication of source code and other documents, the deadlines for such publication, the procedure for announcing findings, and potential financial compensation for discovering important vulnerabilities, are part of the technical requirements and that elaborated measures aim to reflect state-of-the-art technology and align with international good practice.**

> **RECOMMENDATION H.**
>
> ***To clarify in the REA which forms of control may also be carried out by members of the interested public—such as qualified civil society experts and national or international experts—and to define the transparency measures necessary to enable such public oversight. These measures should aim to reflect state-of-the-art technology and align with international good practice.***

60. As noted above, the legal framework for internet voting grants national bodies involved in its implementation and supervision the responsibility/power to engage private companies to provide certain services related to the e-voting process. While this complies with the ODIHR ICT Handbook's specification that "election officials must be responsible for the overall conduct of elections, including the oversight of NVT." The handbook further elaborates that "[i]f NVT involves technology supplied by private vendors, the roles and responsibilities of these vendors must be clearly defined, including crisis management responsibilities."[48] **As a matter of good governance, it is recommended that the REA clarify the general conditions for outsourcing internet voting tasks to private vendors and the respective responsibilities of the NEC, SEO, and vendors. This amendment should be drafted in line with CoE recommendations to ensure that the SEO and NEC fully retain ultimate responsibility for the e-voting process.**

61. When it comes to internet voting, the Academy of Science Cybersecurity Committee, created in 2023, is another important stakeholder.[49] In 2023-24, the focus of its work was on election risks, including paper-based voting and electronic voting from personal computers and mobile devices, in a comparative context. The aim was to create a risk analysis methodology and an initial threat catalogue. The committee assessed 30 threats, of which six were published;[50] the complete list was handed to the SEO, NEC and RIA (June 2024).

62. The committee adopted a methodology corresponding to international practices of modern risk management ("impact - likelihood of threats" methodology). The risk analysis highlights several medium-level threats, including disinformation campaigns that target the credibility of e-voting systems, which can seriously undermine public confidence, especially when they spread claims about vote manipulation or loss of secrecy. Relatedly, the analysis states that

---

48 See ODIHR Handbook for the Observation of Information and Communication Technologies (ICT) in Elections (2024), paragraph 2.1.6.

49 See the Committee's minutes and documents.

50 See the Election Technology Risk Analysis prepared by the Cyber Security Committee of the Academy of Sciences.

persistent public criticism of e-voting—if not effectively countered—could lead to political pressure to restrict or abandon it altogether, reducing voter choice.

63. Another concern lies in the authenticity and integrity of mobile voting applications (m-voting), as, according to the NEC's assessment, current auditing procedures are not robust enough to verify apps distributed through platforms like Apple's App Store or Google Play. Furthermore, the analysis suggests that certain technical stages of the e-voting process are inherently un-auditable due to protocol limitations and third-party dependencies. Even where auditing is technically possible, existing guidelines may leave critical steps unchecked, depending heavily on the diligence and capabilities of individual auditors. Finally, the commission notes the risk of internet connectivity failures during elections, which could disrupt vote transmission or system functionality, particularly affecting voters abroad.

64. **While, positively, the REA provides for a risk assessment (§48[7]), for legal clarity, it is recommended that legislators define the responsibilities for organising the risk assessment and treatment of the risk, as well as for deciding on the adequacy of mitigation measures and the acceptability of the remaining risks, prior to each election. Furthermore, the REA should clarify the general criteria for risk assessment, including the transparency of assessment results, as well as the budget required for this exercise. Trust assumptions on which internet voting relies should be discussed as part of the risk assessment. A more detailed regulation of risk assessment should form part of the technical requirements, as discussed in paragraph 58.**

65. Despite tight controls and risk mitigation measures, there is always a risk that parts of the system may not function correctly (i.e., it may not be immediately apparent whether votes have been lost, added, or changed along the purely electronic path from the voting devices through the digital ballot box to the result announced online). Such changes can be caused not only by intentional manipulation but also by unknown software bugs that can be introduced through updates or malware. The solution proposed by researchers is end-to-end verifiability, which enables checking that the final result aligns with the voters' will, even if parts of the system fail to function as required.[51] The CoE's Recommendations and ODIHR's Handbook for the Observation of ICT in elections note that end-to-end verifiability comprises individual and universal verifiability, or cast-as-intended, recorded-as-cast and tallied-as-recorded without compromising the secrecy of the vote as well as the voters' eligibility verifiability.[52] The verification that the vote was cast and stored as intended may be done by the voter, while universal verifiability should ensure the integrity of the electronic ballot box (that no votes were altered, removed, illegally added or resorted) and that the results are correctly counted and reported. **In light of the above, it is recommended that the legislator defines in the REA the legal requirements of individual verifiability as well as of coercion-resistance related to it, and universal verifiability, including who can conduct universal verifiability checks, taking into account the definitions from CoE Europe Recommendation Rec(2017)5 and considering the voting system as a whole. The detailed technical implementation of these legal requirements should be included as part of the technical requirements referenced above. As state-of-the-art universal verifiability checks provide a possibility to really**

---

51 For example, see a recent study: A Study of Mechanisms for End-to-End Verifiable Online Voting, 2024

52 It should be underlined that ODIHR's use of the term end-to-end verifiability is not meant to include individual verifiability of whether the vote was counted as recorded, as this could constitute a definitive possibility for voters to prove for whom they voted, thus undermining the secrecy of the vote.

"observe" internet voting, it is recommended that the legislator consider conditions for involving observers to conduct universal verifiability checks.[53] It is further recommended to clarify what additional information on the system and procedures will be provided to voters, including details on the control options available to voters (individual verifiability checks), as well as the possibility for voters to test the system.

RECOMMENDATION I.

To define in the REA the legal requirements for individual verifiability and its associated coercion-resistance measures, as well as for universal verifiability. This should include specifying who is entitled to conduct universal verifiability checks, taking into account the characteristics of the voting system. Additionally, consideration should be given to the conditions under which observers may be involved in conducting such verifiability checks.

66. An important aspect that contributes to instilling trust in elections is the participation of observers who, in the context of internet voting, may have specialised backgrounds and proficiencies to understand the complexities of such voting infrastructure and processes. For this reason, the above-noted recommendations propose involving observers in the public discussions of establishing legal requirements for internet voting, defining technical requirements, implementing universal verification checks, and establishing independent controls by the public. Additionally, ODIHR's election observation reports on Estonian elections have proposed various recommendations to enhance transparency and bolster public trust. **In this regard, it is worth reiterating ODIHR's 2023 recommendation aimed at increasing trust in internet voting: "The election authorities should proactively address all concerns raised by election stakeholders who distrust the results of internet voting."[54] This could include both substantive responses to communications that raise concerns as well as periodic voter education campaigns.**

67. Over the years, some civil society observers have filed numerous complaints with the NEC regarding the integrity of the internet voting process. These complaints cited a lack of opportunity to independently verify the process and alleged irregularities or weaknesses in the system. There has been a recent Supreme Court challenge regarding the levels of access for civil society observers when joining meetings remotely.[55] The Supreme Court, which is the final instance in election-related cases and the constitutional review authority, has repeatedly ruled inadmissible appeals lodged by observers, including those that call for constitutional review, on the grounds that observers only have a right to lodge complaints on violations of their right to observe, and do not have the right to file general complaints about the electoral process.[56] In its judgements, the Court stated that while observers cannot file complaints on issues of e-voting, they may seek clarifications from the electoral authorities, present their opinions in reports, draw public attention to their concerns, or submit their views to the legislature during the review of the relevant law. The Court has also ruled that the right to observe is passive; that is, the

---

53 Currently, observers in Estonia are only allowed to conduct "visual observation", which is insufficient for generating observer accounts that the internet voting was conducted accurately. Regarding Supreme Court decisions on this issue, see the discussion in paragraph 65.

54 ODIHR EOM Final Report, 5 March 2023 Parliamentary Elections.

55 See Supreme Court ruling 5-25-3 of 11 April 2025.

56 §70 REA provides that "an individual, a candidate or a political party who finds that their rights have been infringed by a contested act has the right to file a complaint."

observers are not granted any right to conduct verifiability checks on the internet voting system.[57] These judgements, even if based on a reasonable interpretation of the applicable law, essentially prevent observers from meaningfully observing the e-voting process and deny effective legal remedy in their claims of irregularities and challenges to the constitutionality of the applicable regulations.

68. **The legislation should define how to address irregularities identified by universal verifiability checks to ensure an effective remedy. Ideally, such dispute resolution should be regulated as part of the system's functioning and made clear in the technical requirements.** Depending on the exact form that universal verifiability may take in this case, legal dispute resolution mechanisms may need to be introduced or expanded since, so far, observers have no legal possibility of introducing legal complaints in the public interest concerning the internet voting system (nor for any observed violation of electoral legislation). **In line with international good practice to grant as widely as possible standing to lodge complaints, consideration should be given to legislating the right and process to lodge complaints on irregularities identified by observers, allowing them to file complaints in the public interest.[58] In this regard, the legislator would also need to consider the complexities of internet voting when establishing appropriate deadlines, required proofs, and other necessary details for the submission and resolution of such complaints and appeals.[59]**

RECOMMENDATION J.

To consider introducing legislation that establishes the right and procedure for lodging complaints regarding internet voting related irregularities identified by observers, including the possibility for such complaints to be filed in the public interest. In this context, the legislator should also address the specific complexities of internet voting when determining appropriate deadlines, evidentiary requirements, and procedures for the submission, examination, and resolution of such complaints and appeals.

69. The 2001 Penal Code, Subchapter 3 on Offences against Freedom of Election, does not include offences tailored to internet voting. The provisions on cyber-related offences also do not

---

57 §19^4(1) REA provides that "everyone has the right to observe the acts and procedures of the National Electoral Commission and election managers". Other provisions stipulate the public nature of a limited number of aspects of e-voting, specifically §483, which outlines the setup of an encryption key for e-votes and a vote-opening key for decrypting the votes, and §601, which governs e-vote counting. Asserted insufficiencies of current practice are highlighted in a petition by Civil society observers from the NGO Fair Elections, "Demand for observable electronic voting", of 31 March 2023, presented to the Parliament on 4 July 2023.

58 A reasonable quorum may, however, be imposed for appeals by voters on the results of elections. See Venice Commission Code of Good Practice in Electoral Matters, Explanatory report, pp. 38-40.

59 §72 REA establishes a three-day deadline for filing complaints with the NEC; such complaints must be resolved within five days. Under §38(1) of the Constitutional Review Procedure Act, election-related appeals to the Supreme Court must be lodged within three days and per §44(1), the Court has up to seven days to adjudicate the case (and up to four months as per §45(3) if the matter raises a constitutional question). The Venice Commission Code of Good Practice in Electoral Matters (Explanatory report, 3.3) states: "Time limits must […] be long enough to make an appeal possible, to guarantee the exercise of rights of defense and a reflected decision. A time limit of three to five days at first instance (both for lodging appeals and making rulings) seems reasonable for decisions to be taken before the elections. It is, however, permissible to grant a little more time to Supreme and Constitutional Courts for their rulings."

establish specific crimes related to electronic voting. **As a deterrent to potential abuse of the internet voting process or system and to ensure that such malfeasance can be effectively prosecuted, it is recommended to consider updating criminal law provisions to establish offences and dissuasive, proportionate sanctions specific to all stages of the internet voting process.**

RECOMMENDATION K.

To consider updating criminal law provisions to establish offences and dissuasive, proportionate sanctions specific to all stages of the internet voting process.

3.4. Judgments on the Constitutionality of Internet Voting

70. Paragraph 60 of the Constitution states that parliamentary elections are "universal, uniform and direct" and that "voting is by secret ballot".[60] Ensuring the constitutionality of internet voting involves a chain of controls: the compliance of legal requirements on internet voting with constitutional principles is assessed by the authorities that introduce the legal requirements and/or through controls of constitutionality by the Supreme Court; the conformity of technical requirements with legal requirements is ensured, first and foremost, by involving all mentioned stakeholders as recommended above (representative groups of experts, including academia and civil society experts), peers, including international ones, and by deciding on technical requirements in a consensual manner, based on state of the art technology standards and good practice; the conformity of the internet voting system and procedures with technical requirements is ensured through controls and risk assessments. The conformity of the actual use of internet voting during voting and counting is ensured mainly through individual and universal verifiability checks.

71. In Estonia, evaluations of the constitutional conformity of acts can be initiated by the President of the Republic, the Chancellor of Justice, or the Supreme Court in the context of a legal case, and the evaluation is conducted by the Supreme Court. The President may refrain from promulgating a law adopted by the Parliament and return it to the Parliament for a new debate and decision or shall propose to the Supreme Court to declare the law unconstitutional (§107 Cst.). The Chancellor of Justice reviews the acts of general application of the legislature and the executive for conformity with the Constitution and laws (§139 Cst.), and if they find that an act of general application adopted by the legislature or the executive conflicts with the Constitution or a law, they are bound to propose to the Supreme Court to declare the act invalid (§142 Cst.). When adjudicating a matter, a court shall not apply any law or other legal act that is in conflict with the Constitution. The Supreme Court shall declare invalid any law or other legal act that conflicts with the letter and spirit of the Constitution (§151 Cst.).

72. The interpretation of constitutional principles in the context of internet voting has been discussed in judgements issued by the Supreme Court in 2005, 2011, and 2025.[61] The Supreme

---

60 The Constitution (p.156) provides for the same electoral principles with respect to municipal elections.

61 Constitutional judgement 3-4-1-13-05 of 1 September 2005. This judgment addresses the President of the Republic's petition to declare the Local Government Council Election Act Amendment Act unconstitutional. The court ultimately dismissed the petition, upholding the provisions of the Act related to electronic voting. Constitutional judgments 3-4-1-4-11 of 21 March 2011 and 3-4-1-7-11 of 23 March 2011 and judgment 5-25-3 of 11 April 2025.

Court decided in 2005 to interpret the constitutional principles of uniformity and equal treatment to allow for the re-casting of votes in internet voting as a measure to protect against coercion and contribute to ensuring the possibility of secret voting for internet voters. The 2011 Court decisions noted that a prerequisite for declaring the voting results invalid is an established violation of the voter's rights, which in turn raises questions about obtaining proof in internet voting and ensuring verifiability. The 11 April 2025 decision found that the partial limitation placed on an observer's remote attendance was lawful and that the NEC "must assess on a case-by-case basis" whether the information being discussed is sensitive and could endanger system security.

73. Further, in its 2019 and 2023 judgements, the Supreme Court stated that the task of the Parliament is "to stipulate in the electoral laws a sufficiently tight regulation regarding all important issues related to elections, in order to ensure the control of the legislator and the public trust in the elections by means of organisational, procedural and substantive legal requirements".[62] The Supreme Court has repeatedly stated that in matters concerning fundamental rights, all decisions important for the realization of fundamental rights must be made by the legislator. Lesser restrictions on fundamental rights can be imposed by regulation on the basis of precise, clear and proportionate authorisation norms (e.g., delegation to the government). This implies that the legislator should clearly delimit the perimeter of such restrictions. Members of Parliament stated that the 2024 amendments to the REA were intended to address the recent Supreme Court decisions,[63] and were essentially a transfer of existing lower-level e-voting regulations into the legislation; however, they did not constitute a genuinely in-depth, broadly inclusive effort to strengthen the e-voting regulatory framework.

---

62 Constitutional judgments in cases 5-19-18 and 5-19-20 and judgment in case no. 5-23-30 of 27 March 2019, paragraph 83.

63 See press release by Parliament stating that "[t]he Act on Amendments to the Riigikogu Election Act and Amendments to Other Associated Acts eliminates the shortcomings that became apparent in the regulation of online voting in recent elections, and which have also been pointed out by the Supreme Court."