REQUEST FOR PROPOSAL (RFP)

Development of the computer subsystem 'State Registry of Voters' of State Automated Information System 'Elections'

RFP Reference No.:	RfP26/03301
Country:	Republic of Moldova
Issued on:	5 June 2026

Contents

SECTION 1: LETTER OF INVITATION

United Nations Development Programme, hereinafter referred to as UNDP, through "**Strengthening Democratic Resilience in Moldova (EDMITE III)**" Project, hereby invites prospective proposers to submit a proposal for **development of the computer subsystem "State Registry of Voters" of State Automated Information System "Elections"** in accordance with the General Conditions of Contract and the Terms of Reference as set out in this Request for Proposal (RFP).

To enable you to submit a proposal, please read the following attached documents carefully.

Section 1: This Letter of Invitation

Section 2: Instruction to Proposers

Section 3: Data Sheet

Section 4: Evaluation Criteria

Section 5: Terms of Reference

Section 6: Conditions of Contract and Contract Forms

Section 7: Proposal Forms

- **Form A:** Proposal confirmation

- **Form B:** Checklist

- **Form C**: Technical Proposal Submission

- **Form D:** Proposer Information

- **Form E:** Joint Venture/Consortium/Association Information

- **Form F:** Eligibility and Qualification

- **Form G:** Format for Technical Proposal

- **Form H:** Format for CV of Proposed Key Personnel

- **Form I:** Statement of Exclusivity and Availability

- **Form J**: Financial Proposal Submission

- **Form K:** Format for Financial Proposal

- **Form L:** Proposal Security

If you are interested in submitting a proposal in response to this RFP, please prepare your proposal in accordance with the requirements and procedure as set out in this RFP and submit it by the deadline for submission of proposals set out in Section 3: Data Sheet.

Should you be interested to submit a proposal, please log in to the Quantum NextGenERP supplier portal and subscribe to this tender following the instructions in the system user guide. Please search for the tender using search filters, namely **Negotiation ID: UNDP-MDA-01013.** Once subscribed to the tender, you will be able to receive notifications in case of amendments of the tender document and requirements.

Please indicate whether you intend to submit a bid by creating a draft response without submitting directly in the Quantum NextGenERP supplier portal.

Offers must be submitted directly in the Quantum NextGenERP supplier portal following this link: http://supplier.quantum.partneragencies.org/ using the profile you may have in the portal (please log in using your username and password). In case you have never registered before, follow the Supplier Portal Registration Link.

Please note that the access link to the Supplier registered profile is sent from Oracle within up to 3 days. In case you have not received the access link after 3 days since registration, you should address for support to

UNDP at the email address: sc.md@undp.org. In case you encounter errors with registration (e.g. system states Supplier already is registered), you should address for support to UNDP at the email address: sc.md@undp.org.

Computer firewall could block *oracle* or *undp.org extension* and Suppliers might not receive the Oracle notifications. Please turn down any firewalls on your computers to ensure receipt of email notification.

Do not create a new profile if you already have one. Use the forgotten password feature in case you do not remember the password or the username from previous registration.

Should you require further clarifications on the application through the Quantum online portal, kindly contact the Procurement Unit at sc.md@undp.org. Please pay attention that the proposal shall be submitted online through the Quantum system and any proposal sent to the above email shall be disqualified.

Should you require further clarifications on the Request for Proposal, Terms of Reference or other requirements, kindly communicate using the messaging functionality in the portal.

Deadline for Submission of Offers (Date and Time), which is visible in the online procurement system will be final. System will not accept submission of any proposal after that date and time. It is the responsibility of the bidder to make sure that the proposal is submitted prior to this deadline for submission.

Bidders are advised to upload proposal documents and to submit their offer a day prior or well before the date and time indicated under the deadline for submission of Offers. Do not wait until last minute. If Bidder faces any issue during submitting offers at the last minutes prior to the deadline for submission, UNDP may not be able to assist on such a short notice and will not be held liable in such instance. UNDP will not accept any offer that is not submitted directly through the System.

We look forward to receiving your proposal.

UNDP Moldova

SECTION 2: INSTRUCTIONS TO PROPOSERS

GENERAL	
1. Scope	Proposers are invited to submit a proposal for the services specified in Section 5: Terms of Reference, in accordance with this Request for Proposal (RFP). A summary of the scope of the proposal is included in Section 3: Data Sheet. Proposers shall adhere to all the requirements of this RFP, including any amendment made in writing by UNDP. This RFP is conducted in accordance with Policies and Procedures of UNDP which can be accessed at UNDP Programme and Operations Policies and Procedures/Procurement. As part of the bid, it is desired that the Bidder registers at the United Nations Global Marketplace (UNGM) website (www.ungm.org). The Bidder may still submit a bid even if not registered with the UNGM. However, if the Bidder is selected for contract award, the Bidder must register on the UNGM prior to contract signature.
2. Interpretation of the RFP	Any proposal submitted will be regarded as an offer by the proposer and does not constitute or imply the acceptance of the proposal by UNDP. UNDP is under no obligation to award a contract to any proposer as a result of this RFP.
3. Supplier Code of Conduct, Fraud, Corruption, Gifts and Hospitality	All proposers must read the United Nations Supplier Code of Conduct and acknowledge that it provides the minimum standards expected of suppliers to the UN. The Code of Conduct, which includes principles on labour, human rights, environment and ethical conduct may be found at: https://www.un.org/Depts/ptd/about-us/un-supplier-code-conduct Moreover, suppliers should note that certain provisions of the Code of Conduct will be binding on the supplier in the event that the supplier is awarded a contract, pursuant to the terms and conditions of any such contract. UNDP strictly enforces a policy of zero tolerance on proscribed practices, including fraud, corruption, collusion, unethical or unprofessional practices, and obstruction of UNDP vendors and requires all bidders/vendors observe the highest standard of ethics during the procurement process and contract implementation. UNDP's Anti-Fraud Policy can be found at http://www.undp.org/content/undp/en/home/operations/accountability/audit/office_of_audit_andinvestigation.html#anti Bidders/vendors shall not offer gifts or hospitality of any kind to UNDP staff members including recreational trips to sporting or cultural events, theme parks or offers of holidays, transportation, or invitations to extravagant lunches or dinners. In pursuance of this policy, UNDP: Shall reject a proposal if it determines that the selected proposer has engaged in any corrupt or fraudulent practices in competing for the contract in question; Further to the UNDP's vendor sanctions policy, shall declare a vendor ineligible, either indefinitely or for a stated period, to be awarded a contract if at any time it determines that the vendor has engaged in any corrupt or fraudulent practices in competing for, or in executing a UNDP contract.
4. Eligible proposers	Proposers shall have the legal capacity to enter into a binding contract with UNDP. A proposer, and all parties constituting the proposer, may have the nationality of any country with the exception of the nationalities, if any, listed in Section 3: Data Sheet. A proposer shall be deemed to have the nationality of a country if the proposer is a citizen or is constituted, incorporated, or registered and operates in conformity with the provisions of the laws of that country. All proposers found to have a conflict of interest shall be disqualified. Proposers may be considered to have a conflict of interest if they are or have been associated in the past, with a firm or any of its affiliates that have been engaged by UNDP to provide consulting services for the preparation of the design, specifications, Terms of

	Reference, cost analysis/estimation and other documents to be used for the procurement of the services required in the present procurement process; were involved in the preparation and/or design of the programme/project related to the services requested under this RFP; or are found to be in conflict for any other reason, as may be established by, or at the discretion of UNDP and/or are found to be in conflict for any other reason, as may be established by, or at the discretion of UNDP. In the event of any uncertainty in the interpretation of a potential conflict of interest, Bidders must disclose to UNDP, and seek UNDP's confirmation on whether or not such a conflict exists. Similarly, the Bidders must disclose in their proposal their knowledge of the following: If the owners, part-owners, officers, directors, controlling shareholders, of the bidding entity or key personnel are family members of UNDP staff involved in the procurement functions and/or the Government of the country or any Implementing Partner receiving services under this RFP; and All other circumstances that could potentially lead to actual or perceived conflict of interest, collusion or unfair competition practices. Failure to disclose such an information may result in the rejection of the proposal or proposals affected by the non-disclosure. The eligibility of Bidders that are wholly or partly owned by the Government shall be subject to UNDP's further evaluation and review of various factors such as being registered, operated and managed as an independent business entity, the extent of Government ownership/share, receipt of subsidies, mandate and access to information in relation to this RFP, among others. Conditions that may lead to undue advantage against other Bidders may result in the eventual rejection of the Proposal. Proposers shall not be eligible to submit a proposal if at the time of proposal submission: is included in the Ineligibility List, hosted by UNGM, that aggregates information disclosed by Agencies, Funds or Programs of the UN System; is included in the Consolidated United Nations Security Council Sanctions List, including the UN Security Council Resolution 1267/1989 list; is included in the World Bank Corporate Procurement Listing of Non-Responsible Vendors and World Bank Listing of Ineligible Firms and Individuals.
5. Proprietary information	The RFP documents and any Terms of Reference or information issued or furnished by UNDP are issued solely for the purpose of enabling a proposal to be completed and may not be used for any other purpose. The RFP documents and any additional information provided to proposers shall remain the property of UNDP. All documents which may form part of the proposal will become the property of UNDP, who will not be required to return them to your firm.
6. Publicity	During the RFP process, a proposer is not permitted to create any publicity in connection with the RFP.
SOLICITATION DOCUMENTS	
7. Clarification of solicitation documents	Proposers may request clarifications on any of the RFP documents no later than the date indicated in Section 3: Data Sheet. Any request for clarification must be sent in writing in the manner indicated in Section 3: Data Sheet. Explanations or interpretations provided by personnel other than the named contact person will not be considered binding or official. UNDP will provide the responses to clarifications through the method specified in Section 3: Data Sheet. UNDP shall endeavour to provide responses to clarifications in an expeditious manner, but any delay in such response shall not cause an obligation on the part of UNDP to extend the submission date of the proposals, unless UNDP deems that such an extension is justified and necessary.

8. Amendment of solicitation documents	At any time prior to the deadline for proposal submission, UNDP may for any reason, such as in response to a clarification requested by a proposer, modify the RFP in the form of an amendment to the RFP. Amendments will be made available to all prospective proposers. If the amendment is substantial, UNDP may extend the deadline for submission of proposals to give the proposers reasonable time to incorporate the amendment into their proposal.
PREPARATION OF PROPOSALS	
9. Cost of preparation of proposal	The proposer shall bear all costs related to the preparation and/or submission of the proposal, regardless of whether its proposal is selected or not. UNDP shall not be responsible or liable for those costs, regardless of the conduct or outcome of the procurement process.
10. Language	The proposal, as well as any and all related correspondence exchanged by the proposer and UNDP, shall be written in the language(s) specified in Section 3: Data Sheet.
11. Documents establishing eligibility and qualifications of the proposer	The proposer shall furnish documentary evidence of its status as an eligible and qualified vendor, using the forms provided in Section 7 and providing the documents required in those forms. In order to award a contract to a proposer, its qualifications must be documented to UNDP's satisfaction.
11.a Documents comprising the proposal	The proposal bid shall comprise of the following documents and related forms which details are provided in Section 3: Data Sheet: Documents Establishing the Eligibility and Qualifications of the Bidder; Technical Proposal; Financial Proposal; Proposal Security, if required by DS; Any attachments and/or appendices to the Proposal.
12. Technical proposal format and content	The proposer is required to submit a technical proposal using the forms provided in Section 7 and taking into consideration the requirements in the RFP. The technical proposal shall not include any price or financial information. A technical proposal containing material financial information may be declared non-responsive.
13. Financial proposal	The financial proposal shall be prepared using the form provided in Section 7 and taking into consideration the requirements in the RFP. It shall list all major cost components associated with the services, and the detailed breakdown of such costs. Any output and activities described in the technical proposal but not priced in the financial proposal, shall be assumed to be included in the prices of other activities or items as well as in the final total price. Prices and other financial information must not be disclosed in any other place except in the financial proposal.
14. Currencies	All prices shall be quoted in the currency or currencies indicated in Section 3: Data Sheet. Where proposals are quoted in different currencies, for the purposes of comparison of all proposals: UNDP will convert the currency quoted in the proposal into the UNDP preferred currency, in accordance with the UN Operational Rate of Exchange. In the event that UNDP selects a proposal for award that is quoted in a currency different from the preferred currency in Section 3: Data Sheet, UNDP shall reserve the right to award the contract in the currency of UNDP's preference, using the conversion method specified above.
15. Duties and taxes	Article II, Section 7, of the Convention on the Privileges and Immunities provides, inter alia, that the United Nations, including UNDP as a subsidiary organ, is exempt from all direct taxes, except charges for public utility services, and is exempt from customs restrictions, duties, and charges of a similar nature in respect of articles imported or exported for its official use. All proposals shall be submitted net of any direct taxes and any other taxes and duties, unless otherwise specified in Section 3: Data Sheet

16. Proposal validity period	Proposals shall remain valid for the period specified in Section 3: Data Sheet, commencing on the deadline for submission of proposals. A proposal valid for a shorter period may be rejected by UNDP and rendered non-responsive. During the proposal validity period, the proposer shall maintain its original proposal without any change, including the availability of the key personnel, the proposed rates and the total price. In exceptional circumstances, prior to the expiration of the proposal validity period, UNDP may request proposers to extend the period of validity of their proposals. The request and the responses shall be made in writing and shall be considered integral to the proposal. If the proposer agrees to extend the validity of its proposal, it shall be done without any change to the original proposal but will be required to extend the validity of the proposal security, if required, for the period of the extension, and in compliance with Article 17 (Proposal security) in all respects. The proposer has the right to refuse to extend the validity of its proposal without forfeiting the proposal security, if required, in which case, the proposal shall not be further evaluated.
17. Proposal security	A proposal security, if required by Section 3: Data Sheet, shall be provided in the amount and form indicated in the Section 3: Data Sheet. The proposal security shall be valid for a minimum of thirty (30) days after the final date of validity of the proposal. The proposal security shall be included along with the proposal. If a proposal security is required by the RFP but is not found in the proposal, the offer shall be rejected. If the proposal security amount, or its validity period, is found to be less than is required by UNDP, UNDP shall reject the proposal. In the event an electronic submission is allowed in Section 3: Data Sheet, proposers shall include a copy of the proposal security in their proposal and the original of the proposal security must be sent via courier or hand delivery as per the instructions in Section 3: Data Sheet. Unsuccessful proposers' proposal securities will be discharged/returned as promptly as possible but no later than thirty (30) days after the expiration of the period of proposal validity prescribed by UNDP pursuant to Article 16 (Proposal Validity Period). The Proposal security may be forfeited by UNDP, and the proposal rejected, in the event of any, or combination, of the following conditions: If the proposer withdraws its offer during the period of the proposal validity specified in Section 3: Data Sheet, or; In the event the successful Proposer fails: to sign the contract after UNDP has issued an award; or to furnish the performance security, insurances, or other documents that UNDP may require as a condition precedent to the effectivity of the contract that may be awarded to the proposer.
18. Joint Venture, Consortium or Association	If the proposer is a group of legal entities that will form or have formed a Joint Venture (JV), Consortium or Association for the proposal, each such legal entity will confirm in their joint proposal that: they have designated one party to act as a lead entity, duly vested with authority to legally bind the members of the JV, Consortium or Association jointly and severally, and this will be evidenced by a duly notarised agreement among the legal entities, which will be submitted along with the proposal; and if they are awarded the contract, the contract shall be entered into by and between UNDP and the designated lead entity, who will be acting for and on behalf of all the member entities comprising the joint venture. After the deadline for submission of proposal, the lead entity identified to represent the JV, Consortium or Association shall not be altered without the prior written consent of UNDP.

	If a JV, Consortium or Association's proposal is the proposal selected for award, UNDP will award the contract to the joint venture, in the name of its designated lead entity. The lead entity will sign the contract for and on behalf of all other member entities. The lead entity and the member entities of the JV, Consortium or Association shall abide by the provisions of Article 19 (Only one Proposal) herein in respect of submitting only one proposal. The description of the organization of the JV, Consortium or Association must clearly define the expected role of each of the entities in the joint venture in delivering the requirements of the RFP, both in the proposal and the JV, Consortium or Association Agreement. All entities that comprise the JV, Consortium or Association shall be subject to the eligibility and qualification assessment by UNDP. A JV, Consortium or Association, in presenting its track record and experience, should clearly differentiate between: Those that were undertaken together by the JV, Consortium or Association; and Those that were undertaken by the individual entities of the JV, Consortium or Association. Previous contracts completed by individual experts working privately but who are permanently or were temporarily associated with any of the member firms cannot be claimed as the experience of the JV, Consortium or Association or those of its members, but should only be claimed by the individual experts themselves in their presentation of their individual credentials. JV, Consortium or Associations are encouraged for high value, multi-sectoral requirements when the spectrum of expertise and resources required may not be available within one firm.
19. Only one proposal	The proposer (including the individual members of any Joint Venture) shall submit only one proposal, either in its own name or as part of a Joint Venture. Proposals submitted by two (2) or more proposers shall all be rejected if they are found to have any of the following: they have at least one controlling partner, director or shareholder in common; or any one of them receive or have received any direct or indirect subsidy from the other/s; or they have the same legal representative for purposes of this RFP; or they have a relationship with each other, directly or through common third parties, that puts them in a position to have access to information about, or influence on the proposal of another proposer regarding this RFP process; they are subcontractors to each other's proposal, or a subcontractor to one proposal also submits another proposal under its name as lead proposer; or some key personnel proposed to be in the team of one proposer participates in more than one proposal received for this RFP process. This condition relating to the personnel, does not apply to subcontractors being included in more than one proposal.
20. Alternative proposals	Unless otherwise specified in Section 3: Data Sheet, alternative proposals shall not be considered. If submission of alternative proposals is allowed in Section 3: Data Sheet, a proposer may submit an alternative proposal, but only if it also submits a proposal conforming to the RFP requirements. Where the conditions for its acceptance are met, or justifications are clearly established, UNDP reserves the right to award a contract based on an alternative proposal. If multiple/alternative proposals are being submitted, proposer must create an alternate response directly in the system and upload all attachments relevant to the alternate proposal separately together with the alternate response.
21. Pre-proposal conference	When appropriate, a pre-proposal conference will be conducted at the date, time and location and according to any instructions specified in Section 3: Data Sheet.

	If it is stated in Section 3: Data Sheet that the pre-proposal conference is mandatory, a Proposer which does not attend the pre-proposal conference shall become ineligible to submit a proposal under this RFP. If it is stated in Section 3: Data Sheet that the pre-proposal conference is not mandatory, non-attendance shall not result in disqualification of an interested proposer. UNDP will not issue any formal answers to questions from proposers regarding the RFP or proposal process during the pre-proposal conference. All questions shall be submitted in accordance with Article 38 (Clarification of Proposals). The pre-proposal conference shall be conducted for the purpose of providing background information only. Without limiting Article 24 (Proposers responsibility) proposers shall not rely upon any information, statement or representation made at the pre-proposal conference unless that information, statement or representation is confirmed by UNDP in writing. Minutes of the pre-proposal conference will be disseminated as specified in Section 3: Data Sheet. No verbal statement made during the conference shall modify the terms and conditions of the RFP, unless specifically incorporated in the minutes of the proposer's conference or issued/posted as an amendment to RFP.
22. Site inspection	When appropriate, a site inspection will be conducted at the date, time and location and according to any instructions specified in Section 3: Data Sheet. If it is stated in Section 3: Data Sheet that the site inspection is mandatory, a proposer which does not attend the site inspection shall become ineligible to submit a proposal under this RFP. If it is stated in Section 3: Data Sheet that the site inspection is not mandatory, non-attendance, shall not result in disqualification of an interested proposer. Proposers participating in a site inspection shall be responsible for making and obtaining any visa arrangements that may be required for the proposers to participate in a site inspection. Prior to attending a site inspection, proposers shall execute an indemnity and a waiver releasing UNDP in respect of any liability that may arise from: loss of or damage to any real or personal property; personal injury, disease or illness to, or death of, any person; financial loss or expense, arising out of the carrying out of that site inspection; and transportation by UNDP to the site (if provided) as a result of any accidents or malicious acts by third parties. UNDPwill not issue any formal answers to questions from proposers regarding the RFP or solicitation process during a site inspection. All questions shall be submitted in accordance with Article 7 (Clarification of solicitation documents). A site inspection will be conducted for the purpose of providing background information only. Without limiting Article 24 (Proposers Responsibility), proposers shall not rely upon any information, statement or representation made at a site inspection unless that information, statement or representation is confirmed by UNDP in writing.
23. Errors or omissions	Proposers shall immediately notify UNDP in writing of any ambiguities, errors, omissions, discrepancies, inconsistencies or other faults in any part of the RFP, with full details of those ambiguities, errors, omissions, discrepancies, inconsistencies or other faults. Proposers shall not benefit from such ambiguities, errors, omissions, discrepancies, inconsistencies or other faults.
24. Proposers responsibility to inform themselves	Proposers shall be responsible for informing themselves in preparing their proposal. In this regard, proposers shall ensure that they: examine and fully inform themselves in relation to all aspects of the RFP, including the Contract and all other documents included or referred to in this RFP; review the RFP to ensure that they have a complete copy of all documents;

	obtain and examine all other information relevant to the project and the scope of the requirements available on reasonable enquiry; verify all relevant representations, statements and information, including those contained or referred to in the RFP or made orally during any clarification meeting or site Inspection or any discussion with UNDP, its employees or agents; attend any pre-proposal conference if it is mandatory under this RFP; fully inform and satisfy themselves as to requirements of any relevant authorities and laws that apply, or may in the future apply, to the supply of the services; and form their own assessment of the nature and extent of the services required as included in Section 5: Terms of Reference and properly account for all requirements in their proposal. Proposers acknowledge that UNDP, its directors, employees and agents make no representations or warranties (express or implied) as to the accuracy, currency or completeness of this RFP or any other information provided to the proposers.
25. No material change(s) in circumstances	The proposer shall inform UNDP of any change(s) of circumstances arising during the RFP process, including but not limited to: a change affecting any declaration, accreditation, license or approval; major re-organisational changes, company re-structuring, a take-over, buy-out or similar event(s) affecting the operation and/or financing of the proposer or its major sub-contractors; a change to any information on which UNDP may rely in assessing proposals.
SUBMISSION AND OPENING OF PROPOSALS	
26. Instruction for proposal submission	The proposer shall submit a complete proposal in the format and comprising the documents and forms in accordance with requirements in Section 3: Data Sheet. The proposal shall be delivered according to the method specified in Section 3: Data Sheet. The proposal shall be submitted by the proposer or person(s) duly authorized to commit the proposer. The authorization shall be communicated through a document evidencing such authorization issued by the legal representative of the proposing entity, or, if requested, a Power of Attorney, accompanying the proposal. Proposers must be aware that the mere act of submission of a proposal, in and of itself, implies that the proposer fully accepts the UNDP General Conditions of Contract.
26 a. Online submission	Electronic submission through online portal shall be governed as follows: Electronic files that form part of the proposal must be in accordance with the format and requirements indicated in DS; The Technical Proposal and the Financial Proposal files MUST BE COMPLETELY SEPARATE and each of them must be uploaded individually and clearly labelled. The Financial Proposal file must be uploaded separately only in the commercial section of the RFP in the system. encrypted with a password so that it cannot be opened nor viewed until the password is provided. Documents which are required to be in original form (e.g. Bid Security, etc.) must be sent via courier or hand delivery as per the instructions in DS. Detailed instructions on how to submit, modify or cancel a bid in the online portal are provided in the system Bidder User Guide made available in the procurement notice site and in the portal.
27. Deadline for Submission of Proposals and Late Proposals	Complete proposals must be received by UNDP in the manner, and no later than the date and time, specified in Section 3: Data Sheet. If any doubt exists as to the time zone in which the Proposal should be submitted, refer to http://www.timeanddate.com/worldclock/. It shall be the sole responsibility of the proposers to ensure that their proposal is received by the closing date and time. UNDP shall accept no responsibility for proposals that arrive late due to any technical issues and shall only recognise the actual date and time that the proposal was received by UNDP.

	UNDP may, at its discretion, extend this deadline for the submission of proposals by amending the solicitation documents in accordance with Article 8 (Amendment of solicitation documents). In this case, all rights and obligations of UNDP and proposers subject to the previous deadline will thereafter be subject to the new deadline as extended.
28. Withdrawal, substitution and modification of proposals	A proposer may withdraw or modify its proposal after it has been submitted at any time prior to the deadline for submission directly in the system following the instructions provided in the user guide. However, after the deadline for proposal submission, the proposals shall remain valid and open for acceptance by UNDP for the entire proposal validity period, as may be extended.
29. Storage of proposals	Proposals received are kept confidential and unopened in the system as part security protocols built in the system until the proposal opening date stated in Section 3: Data Sheet.
30. Proposal opening	There is no mandatory public bid opening for RFPs however UNDP may at its discretion sent a public bid opening report from the system only to suppliers who successfully submitted a proposal. The report will include only the names of the companies but not the financial proposal.
31. Late proposals	Any proposal received by UNDP after the deadline for submission of proposals will be destroyed unless the proposer requests that it be returned and assumes the responsibility and expenses for the re-possession of the returned proposal documents. In exceptional circumstances, late proposals may be accepted if it is determined that the submission was sent in ample time prior to the proposal closing and the delay could not be reasonably foreseen by the proposer or were due to force majeure.
EVALUATION OF PROPOSALS	
32. Confidentiality	Information relating to the examination, evaluation, and comparison of proposals, and the recommendation of contract award, shall not be disclosed to proposers or any other persons not officially concerned with such process, even after publication of the contract award. Any effort by a proposer or anyone on behalf of the proposer to influence UNDP in the examination, evaluation and comparison of the proposals or contract award decisions may, at UNDP's decision, result in the rejection of its proposal and may subsequently be subject to the application of prevailing UNDP's vendor sanctions procedures.
33. Evaluation of proposals	UNDP shall evaluate a proposal using only the methodologies and criteria defined in this RFP. No other criteria or methodology shall be permitted. UNDP shall conduct the evaluation solely on the basis of the submitted technical and financial proposals. Evaluation of proposals shall be undertaken in the following steps: Preliminary examination Evaluation of minimum eligibility and qualification (if pre-qualification is not done) Evaluation of technical proposals Evaluation of financial proposals.
34. Preliminary examination	UNDP shall examine the proposals to determine whether they are complete with respect to minimum documentary requirements, whether the documents have been properly signed, and whether the proposals are generally in order, among other indicators that may be used at this stage. UNDP reserves the right to reject any proposal at this stage.
35. Evaluation of eligibility and qualification	Eligibility and qualification of the proposer will be evaluated against the minimum eligibility and qualification requirements specified in Section 4: Evaluation Criteria and in Article 4 (Eligible proposers). In general terms, vendors that meet the following criteria may be considered qualified: a) They are not included in the UN Security Council 1267/1989 Committee's list of terrorists and terrorist financiers, and in UNDP's ineligible vendors' list;

	b) They have a good financial standing and have access to adequate financial resources to perform the contract and all existing commercial commitments, c) They have the necessary similar experience, technical expertise, production capacity, quality certifications, quality assurance procedures and other resources applicable to the supply of goods and/or services required; d) They are able to comply fully with the UNDP General Terms and Conditions of Contract; e) They do not have a consistent history of court/arbitral award decisions against the Bidder; and f) They have a record of timely and satisfactory performance with their clients.
36. Evaluation of technical and financial proposals	The evaluation team shall review and evaluate the technical proposals on the basis of their responsiveness to the Terms of Reference and other RFP documents, applying the evaluation criteria, sub-criteria, and point system specified in Section 4: Evaluation Criteria. A proposal shall be rendered non-responsive at the technical evaluation stage if it fails to achieve the minimum technical score indicated in Section 3: Data Sheet. When necessary, and if stated in the Data Sheet, UNDP may invite technically responsive proposers for a presentation related to their technical proposals. The conditions for the presentation shall be provided in the proposal document where required. When necessary, and if stated in the Section 3: Data Sheet, UNDP may invite technically responsive bidders for a presentation related to their technical Proposals. The conditions for the presentation shall be provided in the bid document where required. In the second stage, only the financial proposals of those proposers who achieve the minimum technical score will be opened for evaluation. The evaluation method that applies for this RFP shall be as indicated in Section 3: Data Sheet, which may be either of two (2) possible methods, as follows: (a) the lowest priced method which selects the lowest evaluated financial proposal of the technically responsive Proposers; or (b) the combined scoring method which will be based on a combination of the technical and financial score. When the Data Sheet specifies a combined scoring method, the formula for the rating of the proposals will be as follows: <u>Rating the Technical Proposal (TP):</u> TP Rating = (Total Score Obtained by the Offer / Max. Obtainable Score for TP) x 100 <u>Rating the Financial Proposal (FP):</u> FP Rating = (Lowest Priced Offer / Price of the Offer Being Reviewed) x 100 <u>Total Combined Score:</u> Combined Score = (TP Rating) x (Weight of TP, e.g. 70%) + (FP Rating) x (Weight of FP, e.g., 30%)
37. Post-qualification/Due Diligence	UNDP reserves the right to undertake a post-qualification assessment, aimed at determining, to its satisfaction, the validity of the information provided by the proposer. Such exercise shall be fully documented and may include, but need not be limited to, all or any combination of the following: Verification of accuracy, correctness and authenticity of information provided by the proposer; Validation of extent of compliance to the RFP requirements and evaluation criteria based on what has so far been found by the evaluation team; Inquiry and reference checking with Government entities with jurisdiction on the proposer, or with previous clients, or any other entity that may have done business with the proposer; Inquiry and reference checking with previous clients on the performance on on-going or completed contracts, including physical inspections of previous works, as deemed necessary;

	Physical inspection of the proposer's offices, branches or other places where business transpires, with or without notice to the proposer; Other means that UNDP may deem appropriate, at any stage within the selection process, prior to awarding the contract.
38. Clarification of proposals	UNDP may request clarification or further information in writing from the proposers at any time during the evaluation process. The proposers' responses shall not contain any changes regarding the substance or price of the proposal, except to confirm the correction of arithmetic errors discovered by UNDP in the evaluation of the proposals, in accordance with Instructions to Proposers Article 23 (Errors or omissions). UNDP may use such information in interpreting and evaluating the relevant proposal but is under no obligation to take it into account. Any unsolicited clarification submitted by a proposer in respect to its proposal which is not a response to a request by UNDP, shall not be considered during the review and evaluation of the proposals.
39. Responsiveness of proposal	UNDP's determination of a proposal's responsiveness is to be based on the contents of the proposal itself. A substantially responsive proposal is one that conforms to all the terms, conditions, TOR and other requirements of the RFP without material deviation, reservation, or omission. A material deviation, reservation, or omission is one that: affects in any substantial way the scope, quality, or performance of the services specified in the contract; or limits in any substantial way, inconsistent with the solicitation documents, UNDP's rights or the proposer's obligations under the contract; or if rectified would unfairly affect the competitive position of other proposers presenting substantially responsive proposals. If a proposal is not substantially responsive, it shall be rejected by UNDP and may not subsequently be made responsive by the proposer by correction of the material deviation, reservation, or omission.
40. Nonconformities, reparable errors and omission	Provided that a proposal is substantially responsive, UNDP may waive any non-conformities or omissions in the proposal that, in the opinion of UNDP, do not constitute a material deviation. These are a matter of form and not of substance and can be corrected or waived without being prejudicial to other proposers. Provided that a proposal is substantially responsive UNDP may request the proposer to submit the necessary information or documentation, within a reasonable period, to rectify nonmaterial nonconformities or omissions in the proposal related to documentation requirements. Such omission shall not be related to any aspect of the price of the proposal. Failure of the proposer to comply with the request may result in the rejection of its proposal. For financial proposals that have been opened, UNDP shall check and correct arithmetical errors as follows: if there is a discrepancy between the unit price and the line-item total that is obtained by multiplying the unit price by the quantity, the unit price shall prevail and the line item total shall be corrected, unless in the opinion of UNDP there is an obvious misplacement of the decimal point in the unit price; in which case, the line item total as quoted shall govern and the unit price shall be corrected; if there is an error in a total corresponding to the addition or subtraction of subtotals, the subtotals shall prevail, and the total shall be corrected; and if there is a discrepancy between words and figures, the amount in words shall prevail, unless the amount expressed in words is related to an arithmetic error, in which case the amount in figures shall prevail. If the proposer does not accept the correction of errors, its proposal shall be rejected, and its proposal security may be forfeited.
41. Right to accept any proposal and to	UNDP reserves the right to accept or reject any proposals, and to annul the proposal process and reject all proposals at any time prior to contract award, without thereby

reject any or all proposals	incurring any liability to the affected proposer or proposers or any obligation to inform the affected proposer or proposers of the grounds for UNDP's action. UNDP shall not be obliged to award the contract to the lowest priced offer.
AWARD OF CONTRACT	
42. Award criteria	Prior to expiration of the proposal validity, UNDP shall award the Contract to the qualified proposer based on the award criteria indicated in Section 3: Data Sheet.
43. Right to vary requirement at time of award	At the time the Contract is awarded, UNDP reserves the right to increase or decrease the quantity of services originally specified by up to a maximum twenty-five per cent (25%) of the total offer, without any change in the unit price or other terms and conditions and the solicitation document.
44. Notification of award	Prior to the expiration of the period of proposal validity, UNDP will notify the successful proposer in writing by email, fax or post, that its proposal has been accepted. Please note that the proposer, if not already registered at the appropriate level in UNGM, will be required to complete the vendor registration process on the UNGM prior to the signature and finalization of the contract.
45. Debriefing	In the event that a proposer is unsuccessful, the proposer may request a debriefing from UNDP. The purpose of the debriefing is to discuss the strengths and weaknesses of the proposer's submission, in order to assist the proposer in improving its future proposals for UNDP procurement opportunities. The content of other proposals and how they compare to the proposer's submission shall not be discussed.
46. Publication of contract award	UNDP will publish the contract award on UNDP Procurement Notices website https://procurement-notices.undp.org/view_awards.cfm which is linked to the United Nations Global Marketplace, with the RFP Reference number, the information of the awarded proposer's company name, contract amount or LTA and the date of the contract.
47. Contract Signature	Within fifteen (15) days from the date of receipt of the Contract, the successful Bidder shall sign and date the Contract and return it to UNDP. Failure to do so may constitute sufficient grounds for the annulment of the award, and forfeiture of the Bid Security, if any, and on which event, UNDP may award the Contract to the Second highest rated or call for new Bids.
48. Contract Type and General Terms and Conditions	The types of Contract to be signed and the applicable UNDP Contract General Terms and Conditions, as specified in Data Sheet, can be accessed at http://www.undp.org/content/undp/en/home/procurement/business/how-we-buy.html
49. Performance security	The successful Proposer, if so specified in Section 3: Data Sheet shall furnish a Performance Security in the amount and form specified herein: https://popp.undp.org/_layouts/15/WopiFrame.aspx?sourcedoc=/UNDP_POPP_DOCUMENT_LIBRARY/Public/PSU_Solicitation_Performance%20Guarantee%20Form.docx&action=default, within the specified number of days after receipt of the Contract from UNDP. Banks issuing performance securities must be acceptable to the UNDP comptroller, i.e. banks certified by the central bank of the country to operate as a commercial bank. The Performance Security form is available here. . UNDP shall promptly discharge the proposal securities of the unsuccessful proposers pursuant to Article 17 (Proposal security). Failure of the successful proposer to submit the above-mentioned Performance Security or sign the Contract shall constitute sufficient grounds for the annulment of the award and forfeiture of the proposal security. In that event UNDP may award the contract to the next lowest ranked proposer.
50. Bank guarantee for advance payment	Except when the interests of UNDP so require, it is UNDP's standard practice not to make advance payment(s) (i.e., payments without having received any outputs). If an advance payment is allowed as per Section 3: Data Sheet, and if specified there, the proposer shall submit a Bank Guarantee in the full amount of the advance payment using this bank guarantee form available at :

	https://popp.undp.org/_layouts/15/WopiFrame.aspx?sourcedoc=/UNDP_POPP_DOCUMENT_LIBRARY/Public/PSU_Contract%20Management%20Payment%20and%20Taxes_Advanced%20Payment%20Guarantee%20Form.docx&action=default. Banks issuing bank guarantees must be acceptable to the UNDP comptroller, i.e. banks certified by the central bank of the country to operate as a commercial bank.
51. Liquidated Damages	If specified in Section 3: Data Sheet, UNDP shall apply Liquidated Damages for the damages and/or risks caused to UNDP resulting from the Contractor's delays or breach of its obligations as per the Contract. The payment or deduction of such liquidated damages shall not relieve the Contractor from any of its other obligations or liabilities pursuant to any current contract or purchase order.
52. Proposal protest	Any proposer that believes to have been unjustly treated in connection with this proposal process or any contract that may be awarded as a result of such proposal process may submit a complaint to UNDP. The following link provides further details regarding UNDP vendor protest procedures: http://www.undp.org/content/undp/en/home/procurement/business/protest-and-sanctions.html
53. Other Provisions	In the event that the Bidder offers a lower price to the host Government (e.g. General Services Administration (GSA) of the federal government of the United States of America) for similar goods and/or services, UNDP shall be entitled to the same lower price. The UNDP General Terms and Conditions shall have precedence. UNDP is entitled to receive the same pricing offered by the same Contractor in contracts with the United Nations and/or its Agencies. The UNDP General Terms and Conditions shall have precedence. The United Nations has established restrictions on employment of (former) UN staff who have been involved in the procurement process as per bulletin ST/SGB/2006/15 http://www.un.org/en/ga/search/view_doc.asp?symbol=ST/SGB/2006/15&referer

SECTION 3: DATA SHEET (DS)

The following specific data shall complement, supplement or amend the provisions in Section 2: Instructions to Proposers. In case there is a conflict, the provisions herein shall prevail over those in Section 2: Instructions to Proposers.

Ref. Article in Section 2	Data	Specific Instructions / Requirements
1.	Scope	The reference number of this Request for Proposal (RFP) is **RfP26/03301** The services include provision of **development of the computer subsystem "State Registry of Voters" of State Automated Information System "Elections"** as further described in Section 5 of this RFP.
2.	Eligible proposers	Proposers from all countries are eligible to participate in this proposal process.
3.	Clarification of solicitation documents	Any request for clarification of solicitation documents must be sent directly in the system through **Quantum message functionality**. **ATTENTION: PROPOSALS (OR ANY PART OF IT) SHALL NOT BE SUBMITTED IN THE ABOVE MANNER.**
		Deadline for submitting requests for clarifications / questions: **5 days before the submission deadline**
		Supplemental information to the RFP and responses / clarifications to queries will be posted directly in the system.
4.	Language	All proposals, information, documents and correspondence exchanged between UNDP and the proposers in relation to this solicitation process shall be in **English/Romanian**
5.	Partial proposals	Submitting proposals for parts or sub-parts of the TOR is: **Not allowed**
6.	Currencies	Prices shall be quoted only in the currency indicated in the system: **MDL (Moldovan Leu) for local suppliers** and **USD (US Dollars) for international suppliers.** For evaluation purposes, all the rates shall be recalculated at UN Operational Rate of Exchange indicated on the submission deadline: https://treasury.un.org/operationalrates/OperationalRates.php
7.	Duties and taxes	All prices shall: **Be exclusive of VAT and other applicable indirect taxes.**
8.	Proposal validity period	90 days
9.	Proposal security	**Required in the amount of USD 3,000 (three thousand United States dollars)** The Proposal security will be in the same currency as stipulated in Article 6: Currencies. Acceptable forms of Proposal security: ☒Proposal security form template (bank guarantee) set out in Section 7: Proposal Forms **Important Remarks:**

Ref. Article in Section 2	Data	Specific Instructions / Requirements
		•The Proposal Security shall be valid up to **30 days after the final date of validity of bids**. •The Original Copy of Proposal Security documentation must be physically received by UNDP (10) ten calendar days after the deadline for submission of offers indicated in the Quantum system the latest, and a copy of full Proposal Security documentation must be submitted through Quantum system as part of the online bid. **If Proposal security is not submitted as stipulated above, bid shall be disqualified.** The address for submitting the original Proposal Security documentation is as follows: **UNDP Moldova, #131, 31 August 1989 Street,** **MD-2012, Chisinau, Republic of Moldova** **to the attention of Procurement Unit**
10.	Alternative proposals	Shall not be considered.
11.	Pre-proposal conference	Will be conducted Time and time zone: 10:00 AM Chisinau time Date: 25 June 2026 Venue: https://teams.microsoft.com/meet/329548505314583?p=XdrmZ6dzGFlrTTQMuV Meeting ID: 329 548 505 314 583 Passcode: 4Ts7uo2S Interested bidders should register for the conference. To facilitate registration, prospective bidders are required to send the names and email addresses of their authorized representatives using the "Messages" section in Quantum no later than 24 June 2026. In case bidders face any technical difficulties with Quantum platform, they shall send the above-mentioned information to the following email address: sc.md@undp.org. Please ensure that the subject of the email message is marked as 'PRE-PROPOSAL CONFERENCE FOR RfP26/03301. The pre-proposal conference is: ☒ not mandatory, but highly recommended Minutes of the pre-proposal conference will be disseminated directly in the system.
12.	Site inspection	A site inspection will not be held.
13.	Instructions for proposal submission	Proposals must be **submitted directly in Quantum**. Allowable manner of submitting proposals: • File Format: PDF files only • File names must be clearly indicative of the file content and uploaded in the relevant section as instructed in the system. File names must be in English or in the language specified in this document as the bid language.

Ref. Article in Section 2	Data	Specific Instructions / Requirements
		• All files must be free of viruses and not corrupted. • It is recommended that the entire Proposal be consolidated into as few attachments as possible. • The proposer should receive an email acknowledging receipt of the proposal by the system. • **The Financial Proposal (Forms J and K) shall be submitted directly in the system only in the "Commercial section" of the requirements. Non-compliance with this instruction may result in rejection of the proposal received.**
14.	Deadline for proposal submission	Deadline for proposal submission is **indicated in the portal**. In case of discrepancies between the deadline in the system and deadline indicated elsewhere, the one in the system prevails. **Note that system time zone is in EST/EDT (New York) time zone.**
15.	Proposal Opening	Public proposal opening will **NOT** be held.
16.	Evaluation of technical and financial proposals	Evaluation will be based on: ☒ Combined scoring method using a distribution of 70%-30% Technical proposal - financial proposal The maximum number of technical points is detailed in Section 4: Evaluation Criteria To be substantially compliant, Proposers must obtain a minimum threshold of 70% of maximum points from technical evaluation.
17.	Right to vary requirement at time of award	The maximum percentage by which quantities may be increased or decreased is 25%
18.	Contract award to one or more proposer	UNDP will award a contract to: **One Bidder Only**
19.	Type of contract to be awarded	**Contract Face Sheet** More information can be accessed at http://www.undp.org/content/undp/en/home/procurement/business/how-we-buy.html See Section 6 for link to sample contract.
20.	Expected date for commencement of contract	30 July 2026
21.	Conditions of contract to apply	**UNDP General Terms and Conditions for contracts (goods and/or services)** See Section 6 for link to the contract terms.
22.	Performance Security	Not Required
23.	Advance payment	Not Allowed
24.	Liquidated damages	Will be imposed as follows: Percentage of contract price per week of delay: 2.5% up to a maximum of 10% of the Contract value; after which UNDP may terminate the contract.
25.	Documents to be submitted with your Proposal	a. Company Profile, which should not exceed fifteen (15) pages, covering the company experience, human resources, management and technical capacities, portfolio, demonstrating experience in implementation of projects with similar content and similar complexity;

Ref. Article in Section 2	Data	Specific Instructions / Requirements
		b. Certificate of Incorporation/ Business Registration (in case of JV/Consortium/Association, the documents shall be provided for the leader of the consortium and each partner, if any); c. List of Shareholders and Other Entities Financially Interested in the Firm owning 5% or more of the stocks and other interests, or its equivalent if Bidder is not a corporation including the Certificate from State Register; d. Official Letter of Appointment as local representative, if Bidder is submitting a Bid on behalf of an entity located outside the country; e. A copy of preliminary Agreement in case of Consortium; f. Quality Certificate (e.g., ISO 9001, ISO 20000, ISO/IEC 27001 etc..) and/or other similar certificates, accreditations, awards and citations received by the Bidder, if any; g. Financial Statement (Income Statement and Balance Sheet) for the past 3 years (2025, 2024, 2023) in case of JV/Consortium/Association, the documents shall be provided for the leader of the consortium and each partner, if any); h. Copies of contracts to demonstrate experience in implementation of projects of similar complexity (as specified under Section 4: Evaluation Criteria) in the past five (5) years. i. Statement of Satisfactory Performance from the Top three (3) Clients in terms of Contract Value (in case of JV/Consortium/Association, of the leader of the consortium) for successfully implemented projects (ICT Systems); j. Technical Proposal which shall include at least: - Detailed description of the Methodology, Approach and Implementation Plan (sequence of actions) for the services required in the ToR, with clear distribution of roles and responsibilities of the proposed key personnel. - The methodology shall also include the detailed technical description of the proposed software solution including description of functional and non-functional requirements, including the technological platforms, its performance parameters to be used and relevant constraints, required hardware and any operational restrictions (if any), estimated implementation activities and their duration, approach for providing warranty, maintenance and support services (including owned facilities). - Proposed approach for organizing project implementation, listing all implementation stages and corresponding deliverables; - Implementation Plan (sequence of actions) for the services required in the ToR; - Proposed model for management of change and development requests and the methodology applied for estimating the effort and price to be charged; - Project management organizational chart with clear roles and responsibilities, as well as practices applied to interaction and collaboration within the project, including: project plan management, detailed activity planning, resource management, communication plan, change management, risk, management, deliverable quality management, progress monitoring and reporting, exception management, library management project;

Ref. Article in Section 2	Data	Specific Instructions / Requirements
		k. List of qualified Key Personnel, together with their CVs (as mentioned in Section 4: Evaluation Criteria), attestation certificates (e.g. diplomas, certifications), and relevant training certificates clearly demonstrating compliance with the required qualifications and experience. Statements of Exclusivity and Availability confirming participation in the project at the level and duration specified (signed by the envisaged person) shall also be provided. l. All information regarding any past and current litigation during the last three (3) years, in which the bidder is involved, indicating the parties concerned, the subject of the litigation, the amounts involved, and the final resolution if already concluded; m. Environmental Compliance Certificates, Accreditations, Markings/Labels, and other evidence of the Proposer's practices which contributes to the ecological sustainability of reduction of environment impact (e.g., use of non-toxic substances, recycled raw materials, energy-efficient equipment, reduced carbon emission, etc.); **n. Dully filled in Proposal Forms A-K (as per Section 7: Proposal Forms). Forms A-I, representing the Technical Proposal, shall be submitted directly in the system in the "Technical section" of the requirements.** **o. Forms J and K, representing the Financial Proposal shall be submitted directly in the system only in the "Commercial section" of the requirements. Please, ensure that no other documents are disclosing your financial proposal apart from Forms J and K. Non-compliance with this instruction may result in rejection of the proposal received.** **p. Form L, representing Proposal Security, submitted in original not later than ten (10) days after the submission deadline from tender deadline at the address indicated in Article 9**

SECTION 4: EVALUATION CRITERIA

Preliminary Examination Criteria

All criteria will be evaluated on a **Pass/Fail basis** and checked during Preliminary Examination.

Criteria	Documents to establish compliance
Completeness of the Proposal	All documents requested in Section 2: Instructions to Bidders Articles 11 and 12 have been provided and are complete.
Proposer accepts UNDP General Conditions of Contract as specified in Section 6.	Duly signed and stamped Form C: Technical Proposal Submission has been provided.
Proposal Validity	Duly signed and stamped Form C: Technical Proposal Submission has been provided.
Proposal Security with compliant validity period	Duly signed and stamped compliant to validity Form L: Proposal Security has been provided.
Appropriate signatures	Proposal Forms have been duly signed and stamped.
Power of Attorney [if applicable]	Certified Letter of Appointment and/or power of attorney authorizing the representative of the Bidder to sign bids has been provided.

Minimum Eligibility and Qualification Criteria

Minimum eligibility and qualification criteria will be evaluated on a **Pass/Fail basis**.

If the Proposal is submitted as a Joint Venture, Consortium or Association, each member should meet the minimum criteria, unless otherwise specified.

Eligibility Criteria	Documents to establish compliance
Legal Status: Vendor is a legally registered entity and can ensure rapid local response (including presence of staff) to any of the contract related requests (whether though a local branch or office, through a local consortium partner or a local subcontracted company – all relationships to be documented through official documents and valid contracts submitted with the Proposal).	Form D: Proposer Information
Diversity, Inclusion and Belonging: Proposer belongs to a diverse supplier group, including micro, small or medium sized enterprise, women or youth owned business or other.	Form D: Proposer Information
Eligibility: Vendor is not suspended, nor otherwise identified as ineligible by any UN Organization, the World Bank Group or any other International Organisation in accordance with Section 2 Article 4.	Form C: Technical Proposal Submission
Conflict of Interest: No conflicts of interest in accordance with Section 2 Article 4.	Form C: Technical Proposal Submission
Bankruptcy: The Proposer has not declared bankruptcy, in not involved in bankruptcy or receivership proceedings, and there is no judgment or pending legal action against the vendor that could impair its operations in the foreseeable future	Form C: Technical Proposal Submission

Qualification Criteria	Documents to establish compliance

History of non-performing contracts[1]: Non-performance of a contract did not occur as a result of contractor default within the last 3 years[1].	Form F: Eligibility and Qualification
Litigation History: No consistent history of court/arbitral award decisions against the Proposer for the last 3 years.	Form F: Eligibility and Qualification
Previous Experience:	
Minimum 5 (five) years of experience in developing IT systems. *(For JV/Consortium/Association, TEAM Lead company should meet the requirement).*	Form F: Eligibility and Qualification
Minimum 3 (three) successfully executed ICT project contracts of similar nature and complexity within the last 5 (five) years, including: • At least one project implemented for public and/or government institutions (e.g. central public authorities, state agencies, local authorities, etc.), such as national population registries, social protection registries, electoral management systems; digital public service portals with complex back-office workflows; highly configurable case management systems, document and workflow management systems, etc. • At least one project shall include the experience in integrating systems with national interoperability, authentication, electronic signature, and related government digital platforms and services (such as MConnect, MPass, MSign, or equivalent governmental platforms in other countries). *(For JV/Consortium/Association, TEAM Lead company should meet the requirement).*	Form F: Eligibility and Qualification
Minimum Key Personnel:	
The minimum personnel mandatory for the implementation of the contract: • 1 (one) Project Manager • 1 (one) Business Analyst with Training responsibilities • 1 (one) System Architect • 1 (one) Team Leader acting as Senior Software Developer and responsible for UX/UI compliance • 1 (one) Software Developer with Database Administration responsibilities • 1 (one) Software Developer with DevOps responsibilities • 1 (one) QA Expert • 1 (one) Trainer *Please note: Bidders may include supplementary personnel aligned to their implementation methodology, clearly*	Duly signed CVs and Statements of Exclusivity and Availability, including any other supporting documents, attached to Form H: Format for Technical Proposal

[1] Non-performance, as decided by UNDP, shall include all contracts where (a) non-performance was not challenged by the contractor, including through referral to the dispute resolution mechanism under the respective contract, and (b) contracts that were so challenged but fully settled against the contractor. Non-performance shall not include contracts where Employer's decision was overruled by the dispute resolution mechanism. Non-performance must be based on all information on fully settled disputes or litigation, i.e. dispute or litigation that has been resolved in accordance with the dispute resolution mechanism under the respective contract and where all appeal instances available to the Bidder have been exhausted.

describing responsibilities and reporting lines as part of the technical proposal. Any additional personnel shall comply with the same qualification criteria. *(For JV/Consortium/Association all Parties cumulatively should meet requirement).*	
Financial Standing:	
Liquidity: The Ratio Average current assets / Current liabilities over the last 3 (three) years must be equal or greater than 1. Proposers must include in their Proposal audited balance sheets cover the last 3 (three) years. If CR is less than 1: UNDP shall verify financial capacity of the bidder and has the authority to seek references from concerned parties & banks on the bidder' financial standing. UNDP has the right to reject any bid if submitted by a contractor whom investigation leads to a result that the bidder is not financially capable and/or had serious financial problems. *(For JV/Consortium/Association all Parties cumulatively should meet requirement).*	Copy of audited financial statements for the last 3 (three) years. Form F: Eligibility and Qualification
Turnover: Proposers should have a minimum average annual sales turnover of minimum USD 500,000 for the last 3 (three) years (2023, 2024, 2025). *(For JV/Consortium/Association all Parties cumulatively should meet requirement).*	Copy of audited financial statements for the last 3 (three) years. Form F: Eligibility and Qualification

Technical Evaluation Criteria

Summary of technical proposal evaluation sections		**Points obtainable**
1.	Proposer's qualification, capacity and experience	300
2.	Proposed methodology, approach and implementation plan	400
3.	Key personnel	300
	Total	**1000**

Section 1. Proposer's qualification, capacity and experience		**Points obtainable**
1.1	Reputation of organisation and staff credibility / reliability / industry standing Organization / Company profile – 20 points: Excellent: Organization and staff have an outstanding reputation, proven reliability, and a strong company profile supported by verifiable references and achievements: 20 pts Good: Organization and staff have a very good reputation and reliability, with strong references and a solid company profile: 18 pts Satisfactory: Organization and staff have a good reputation and reliability, with adequate references and company profile: 14 pts	**20**

	Poor: Organization and staff have limited reputation and reliability; references and company profile are weak or incomplete: 8 pts. Very Poor: Organization and staff have very little reputation or credibility; references are minimal or questionable: 2 pts. No submission: No information provided or completely unacceptable: 0 pts.	
1.2	General organisational capability which is likely to affect implementation: management structure, financial stability and project financing capacity, project management controls, extent to which any work would be subcontracted. • Financial stability: sales turnover for the last three years (2023, 2024, 2025) (turnover of 500,000 USD to 800,000 USD – 10 pts.; turnover of 800,001 USD to 1,000,000 USD – 15 pts.; more than 1,000,000 USD – 20 pts. • Project management support mechanism (no – 0 pts, yes 5 pts.) • Project management controls (no – 0 pts, yes 5 pts.)	**30**
1.3	Relevance of specialised knowledge and experience on similar engagements done in the region /country • Minimum 5 (five) years of relevant experience in developing IT systems (5 years – 40 pts., each additional year – 5 pts., up to max 60 pts.) • Minimum 3 (three) successfully executed ICT projects of similar complexity within the last 5 (five) years, where: - At least one project implemented for public and/or government institutions (ex. central public authorities, state agencies, local authorities, etc.) (ex. national population registries, social protection registries, electoral management systems; digital public service portals with complex back-office workflows; highly configurable case management systems, document and workflow management systems, etc.) - At least one project shall include the experience in integrating systems with national interoperability, authentication, electronic signature, and related government digital platforms and services (such as MConnect, MPass, MSign, or equivalent governmental platforms in other countries. (3 contracts – 30 pts., each additional project – 5 pts., up to max 60 pts.) • Demonstrated experience of working with Moldovan public institutions would be a strong advantage (each contract / assignment – 10 pts., up to max. 70 pts.) • Demonstrated experience in the design, development and implementation of IT applications for electoral processes would be an advantage (each contract / assignment – 15 pts., up to max. 30 pts.) • Working experience with UN Agencies and/or other international organizations will be an advantage (no – 0 pts., yes – 10 pts.)	**230**
1.4	Organisation Commitment to Sustainability q. Organisation is compliant with ISO 14001 or ISO 14064 or equivalent – 10 points r. Organisation is a member of the UN Global Compact – 5 points s. Organisation demonstrates significant commitment to sustainability through some other means (for example internal company policy documents on women empowerment, renewable energies or membership of trade institutions promoting such issues) – 5 points	**20**
Total Section 1		**300**

Section 2. Proposed methodology approach and implementation plan	**Points obtainable**

2.1	To what degree does the Proposer understands the objectives, scope, and requirements of the assignment? • Excellent Understanding (60 pts): The proposer demonstrates a comprehensive and in-depth understanding of the assignment, objectives, and expected results; proposal fully reflects ToR requirements and provides strong evidence of the ability to meet and exceed them (100 %) • Good Understanding (54 pts): The proposer demonstrates a good understanding of the assignment; proposal addresses ToR requirements well and provides adequate evidence of capacity to deliver (90%) • Satisfactory Understanding (42 pts): The proposer demonstrates a general understanding of the assignment; proposal addresses most ToR requirements but with some gaps or limited supporting evidence (70%) • Poor Understanding (24 pts): The proposer shows limited understanding of the assignment; proposal addresses ToR requirements superficially and provides weak supporting evidence (40%) • Very poor Understanding (6 pts): The proposer shows very little understanding of the assignment; proposal largely fails to address ToR requirements (10%) • No submission: Information has not been submitted or completely unacceptable: 0 pts	**60**
2.2	Is the proposal clear, and is the sequencing of activities logical, realistic, and conducive to efficient implementation? • Excellent (140 pts): The proposal is clear, well structured, and presents a logical, realistic, and well-sequenced implementation plan. Human and material resources are appropriately allocated and support efficient delivery (100 %) • Good (126 pts): The proposal is clear and structured, with a generally realistic sequence of activities and adequate resource allocation. Minor adjustments could enhance efficiency (90%) • Satisfactory (98 pts): The proposal presents an acceptable structure and activity sequence but includes gaps or assumptions that may affect efficient implementation (70%) • Poor (56 pts): The proposal lacks clarity and coherence in activity sequencing and resource allocation, raising concerns about feasibility (40%) • Very Poor (14 pts): The proposal is poorly structured, with unrealistic sequencing and insufficient resources (10%) • No submission / Unacceptable (0 pts): No implementation plan provided or submission is unacceptable.	**140**
2.3	To what extent are quality assurance procedures and risk mitigation measures adequately defined? • Excellent (60 pts): Quality assurance and risk mitigation mechanisms are clearly defined, comprehensive, and fully integrated into the implementation approach, addressing all relevant technical, operational, and fiduciary risks (100 %) • Good (54 pts): Quality assurance and risk mitigation measures are well defined and cover most relevant risks, with minor gaps that do not significantly affect robustness (90%) • Satisfactory (42 pts): Quality assurance and risk mitigation measures are outlined but lack sufficient detail or coverage of key risks (70%) • Poor (24 pts): Quality assurance and risk mitigation measures are weak, incomplete, or insufficiently linked to implementation risks (40%) • Very Poor (6 pts): Mechanisms are largely inadequate, missing critical elements and failing to address major risks (10%)	**60**

	• No submission / Unacceptable (0 pts): No quality assurance or risk mitigation measures provided or submission is unacceptable.	
2.4	The proposed technical solution is adequate and is compliant with the computer subsystem Registry of Voters's functional and non-functional requirements. • Excellent (140 pts): The proposed technical solution demonstrates a very strong and relevant approach and the Technical Responsiveness Checklist is dully completed and fully responds to the State Registry of Voters requirements (100%) • Good (126 pts): The proposed technical solution demonstrates a sound and relevant approach and the Technical Responsiveness Checklist is dully completed and responds to the Financial Control requirements (90%) • Satisfactory (98 pts): The proposed technical solution demonstrates an acceptable and relevant approach and the Technical Responsiveness Checklist is completed and responds to some extent to the State Registry of Voters requirements (70%) • Poor (56 pts): The proposed technical solution demonstrates a weak and partially relevant approach and the Technical Responsiveness Checklist is not fully completed and partially responds to the State Registry of Voters requirements (40%) • Very Poor (14 pts): The proposed technical solution does not demonstrate a relevant approach and the Technical Responsiveness Checklist not completed and does not respond to the State Registry of Voters requirements (10%) • No submission / Unacceptable (0 pts): Information is missing or does not allow assessment under this criterion.	**140**
Total Section 2		**400**

Section 3. Key Personnel*			**Points obtainable**
3.1	**Project Manager**		**45**
	University degree in Management, Engineering, ICT or another relevant field (bachelor's degree – 2.5 pts., master's degree – 5 pts.)	5	
	At least 5 (five) years of experience in project management of projects on developing IT applications/systems, services, etc. (5 years – 5 pts., each additional year – 2 pts., up to a max. of 15 pts.)	15	
	Experience in at least 2 (two) similar complexity software development projects (two projects – 4 pts., each additional project – 2 pts., up to max 10 pts.)	10	
	Relevant experience in business process analysis (no – 0 pts., yes – 5 pts.)	5	
	Proven certification in Project Management (PMP, PRINCE2, CSM, CBAP / CCBA, ISTQB, AZURE, TOGAF, SAFe, etc.) would be an asset (no – 0 pts., yes – 5 pts.)	5	
	Proficiency in Romanian and English languages (English, Romanian – 2.5 pts. each)	5	
3.2	**Business Analyst with Training responsibilities**		**50**
	University degree in Management, Engineering, ICT or another relevant field (bachelor's degree – 2.5 pts., master's degree – 5 pts.)	5	
	At least 5 (five) years of experience in business analysis (5 years – 4 pts., each additional year – 2 pts., up to a max. of 10 pts.)	10	
	Experience as Business Analyst or similar position in at least 2 (two) software development projects of similar complexity (two projects – 4 pts., each additional project – 2 pts., up to max 10 pts.)	10	
	Relevant certification such as CBAP, General Business Analysis Certifications, Product Ownership or BPM would be an asset (no – 0 pts., yes – 5 pts.)	5	

	Proven experience in delivering user training for information systems in at least 2 (two) projects implemented within the past 3 (three) years (two projects – 4 pts., each additional project – 2 pt., up to max 10 pts.)	10	
	Proven experience in preparing documentation and training materials for end users, including for the UAT process (no – 0 pts., yes – 5 pts.)	5	
	Proficiency in Romanian and Russian languages (Russian, Romanian – 2.5 pts. each)	5	
3.3	**System Architect**		
	University degree in Computer Science or another relevant domain (bachelor's degree – 2,5 pts., master's degree – 5 pts.)	5	
	At least 5 (five) years of professional experience as a System Architect in the design, development and implementation of information systems (5 years – 4 pts., each additional year – 2 pts., up to a max. of 10 pts.)	10	
	Experience as a System Architect in at least 2 (two) projects of similar complexity implemented within the last 3 (three) years (2 projects – 6 pts., each additional project – 2 pts., up to max 10 pts.)	10	**40**
	Experience in unit testing, continuous integration and DevOps practices (no – 0 pts., yes – 5 pts.)	5	
	Certifications in information systems architecture or design (e.g. TOGAF 9, CTA or equivalent) is an asset (each certification – 2,5 pts., up to a max of 5 pts.)	5	
	Proficiency in Romanian and English or Russian languages (Romanian – 2,5 pts., English or Russian – 2,5 pts.)	5	
3.4	**Team Leader acting as Senior Software Developer and responsible for UX/UI compliance**		
	University degree in Computer Science or another relevant domain (bachelor's degree – 2.5 pts., master's degree – 5 pts.)	5	
	At least 5 (five) years of experience in developing information using the proposed technology stack (5 years – 4 pts., each additional year – 2 pts., up to a max. of 10 pts.)	10	
	Participated in at least 2 (two) similar complexity projects in the last 3 (three) years (2 projects – 4 pts., each additional project – 2 pts., up to max 10 pts.)	10	
	Experience in unit / module testing, continuous integration and DevOps practices (no – 0 pts., yes – 5 pts.)	5	**50**
	Experience in information systems integration and in designing and implementing data exchange interfaces (APIs) using SOAP and REST (no – 0 pts., yes – 5 pts.)	5	
	Proven experience in design tools such as Figma (advanced level), FigJam, etc.; or experience in UX principles, wireframing, prototyping and accessibility (WCAG); or experience in collaborating within design systems and maintaining design documentation (no – 0 pts., yes – 5 pts.)	5	
	Certifications in any technology from the proposed technology stack mentioned above is an asset (each certification – 2,5 pts., up to a max of 5 pts.)	5	
	Proficiency in Romanian and English languages (English, Romanian – 2,5 pts. each)	5	
3.5	**Software Developer with Database Administration responsibilities**		
	University degree in Computer Science or another relevant domain (bachelor's degree – 2.5 pts., master's degree – 5 pts.)	5	
	At least 5 (five) years of experience in software development as a Database Developer/Administrator, using the proposed technology stack (5 years – 4 pts., each additional year – 2 pts., up to a max. of 10 pts.)	10	**30**
	Experience in a similar position in at least 2 (two) similar complexity projects in the last 3 (three) years (2 projects – 3 pts., each additional project – 1 pt., up to max 5 pts.)	5	
	Experience in unit testing and continuous integration (no – 0 pts., yes – 5 pts.)	5	

	Certification in database technologies and in the proposed technology stack is an asset (each certification – 2,5 pts., up to a max of 5 pts.)	5	
3.6	**Software Developer with DevOps responsibilities**		
	University degree in Computer Science or another relevant domain (bachelor's degree – 2.5 pts., master's degree – 5 pts.)	5	
	At least 5 (five) years of experience in software development using the proposed technology stack (5 years – 4 pts., each additional year – 2 pts., up to a max. of 10 pts.)	10	
	Experience in a similar position in at least 2 (two) similar complexity projects in the last 3 (three) years (2 projects – 3 pts., each additional project – 1 pt., up to max 5 pts.)	5	**35**
	Experience and competencies in continuous integration and continuous delivery for information systems of similar complexity (no – 0 pts., yes – 5 pts.)	5	
	Experience in unit testing and DevOps practices (no – 0 pts., yes – 5 pts.)	5	
	Certification in continuous integration and continuous delivery (CI/CD) for information systems in the proposed technology stack is an asset (each certification – 2,5 pts., up to a max of 5 pts.)	5	
3.7	**QA Expert**		
	University degree in Computer Science or another relevant domain (bachelor's degree – 2.5 pts., master's degree – 5 pts.)	5	
	At least 5 (five) years of experience in testing information systems (5 years – 2 pts., each additional year – 1 pt., up to a max. of 5 pts.)	5	
	Experience in a similar position in at least 2 (two) similar complexity projects in the last 3 (three) years (2 projects – 3 pts., each additional project – 1 pt., up to max 5 pts.)	5	
	Proven experience in functional and non-functional testing of information systems, in accordance with the methodology proposed (no – 0 pts., yes – 5 pts.)	5	**35**
	Proven experience in performance testing (load and stress testing) and security testing, covering at least the OWASP Top 10 vulnerabilities (no – 0 pts., yes – 5 pts.)	5	
	Proven experience in applying automated testing to information systems (no – 0 pts., yes – 5 pts.)	5	
	Certification in software testing (e.g. ISTQB) and in using the proposed technology stack is an asset (each certification – 2,5 pts., up to a max of 5 pts.)	5	
3.8	**Trainer**		
	Proven experience in organisation and delivery of training on information systems (each training - 1 pt., up to max of 5 pts.)	5	
	Experience in developing user, administrative and architectural documentation (each document – 1 pt., up to max. 5 pts.)	5	**15**
	Experience in the organisation of the UAT process and other types of testing involving end users (each testing - 1 pt., up to max of 5 pts.)	5	
		Total Section 3	**300**

**** For details on the role of the key personnel, please consult Section 5.15 of this RfP.***

SECTION 5: TERMS OF REFERENCE

1. General information

The Central Electoral Commission (CEC) is an independent state body established to implement electoral policy in order to ensure the proper conduct of elections, and to supervise and monitor compliance with the legal provisions on the financing of political parties and electoral campaigns.

The mission of the Central Electoral Commission is to create optimal conditions for the citizens of the Republic of Moldova to freely exercise their constitutional right to vote and to be elected in free and fair elections, including by ensuring compliance with the legislation on the financing of political parties and electoral campaigns.

Under the Electoral Code[2], the *State Register of Voters* (SRV) is a single integrated information system for keeping records of voters, being an integral part of the State Automated Information System 'Elections' (SAISE), designed to collect, store, update and analyse information on citizens of the Republic of Moldova who have reached voting age. Article 60 of the Electoral Code lays down the core organisational and legal requirements for the SRV, how it is formed, administered and updated, as well as the basic requirements regarding the data it contains. Accordingly, the CEC is the holder of the SRV and ensures its administration and updating.

Under the Law on Registers[3] and the Law on Informatisation and State Information Resources, the CEC, as holder, has various duties and responsibilities. Particularly, to ensure the functioning of the SRV, the CEC, by Decision No. 1140 of 28.07.2023[4], approved the Regulation on the State Register of Voters.

Currently, the SRV's functionalities are only partially implemented (covered) by SAISE. Taking into account SAISE's technological limitations, as well as several issues in validating and ensuring the accuracy of data from external sources, the CEC needs to create a complex automated tool, adapted to technical, technological and organisational realities, that will enable compliance with legal requirements for the SRV, while also providing convenient and secure instruments necessary to address data inconsistencies and discrepancies.

Under the Law on Registers, the State Register is the sole official source of data on the objects recorded in it. Data in the register are deemed correct and truthful unless and until proven otherwise, in accordance with the law. The SRV is formed on the basis of information supplied by data providers, such as the Public Services Agency, the Ministry of Justice, the Ministry of Defence and other authorities. In this context, as the holder of the SRV, the CEC is obliged to:

- organise the creation of automated information systems intended for maintaining the register;
- ensure the registration of the objects subject to registration;
- ensure the authenticity, completeness and integrity of the data in the register;
- ensure all recipients have access to the data in the register in line with the law and the rules for keeping registers.

This commitment is implemented with support from the UNDP "Strengthening Democratic Resilience in Moldova" (EDMITE III) Project. This commitment is part of a series of projects and activities designed to ensure the CEC's technological modernisation, alignment with the EU regulatory framework and election-conduct requirements, and citizens' access to information.

[2] https://www.legis.md/cautare/getResults?doc_id=148963&lang=ro
[3] https://www.legis.md/cautare/getResults?doc_id=140170&lang=ro#
[4] https://www.legis.md/cautare/getResults?doc_id=138555&lang=ro

2. Abbreviations and acronyms

Abbreviation	Full name
ADR	Architecture Decision Record
AES	Advanced Encryption Standard
API	Application Programming Interface
DB	Database
BPMN	Business Process Model and Notation
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CEC	Central Electoral Commission of the Republic of Moldova
CERT-GOV-MD	Computer Emergency Response Team - Guvernamental Moldova
CI/CD	Continuous Integration / Continuous Deployment
CIS	Center for Internet Security
COTS	Commercial Off-The-Shelf
CRUD	Create, Read, Update, Delete
CSV	Comma-Separated Values
CUATM	Classifier of Administrative-Territorial Units of Moldova
DDoS	Distributed Denial of Service
DevOps	Development and Operations
DR	Disaster Recovery
EGOV	E-Governance Agency
ETL	Extract, Transform, Load
ERD	Entity-Relationship Diagram
EVO	The integrated government portal EVO. A single access point to public services and to digital interaction with state institutions, intended for citizens, entrepreneurs and the diaspora.
FR	Functional Requirement
GDPR	General Data Protection Regulation (EU Regulation 2016/679)
GIS	Geographic Information System
HA	High Availability
HTML	HyperText Markup Language
HTTPS	HyperText Transfer Protocol Secure
IaaS	Infrastructure as a Service
IdP	Identity Provider
IDNP	State Identification Number (IDNP) (unique 13-digit code)
JSON	JavaScript Object Notation
JWT	JSON Web Token
KPI	Key Performance Indicator
LDAP	Lightweight Directory Access Protocol
MFA	Multi-Factor Authentication
MCloud	Common Government Technology Platform
MConnect	National Interoperability Platform
MLog	National Event Logging Platform
MPass	National Electronic Authentication System

Abbreviation	Full name
MSign	National Electronic Signature System
MTBF	Mean Time Between Failures
mTLS	Mutual Transport Layer Security
MTTR	Mean Time To Recovery
MITC	Ministry of Information Technology and Communications
NFR	Non-Functional Requirement
OAuth2	Open Authorization 2.0
OCI	Open Container Initiative
OGC	Open Geospatial Consortium
OpenID	OpenID Connect
OWASP	Open Web Application Security Project
PaaS	Platform as a Service
PDF	Portable Document Format
PII	Personally Identifiable Information
PM	Project Manager
M	Minutes
PWA	Progressive Web App
QA	Quality Assurance
RACI	Responsible, Accountable, Consulted, Informed
RBAC	Role-Based Access Control
REST	Representational State Transfer
RM	Republic of Moldova
RPO	Recovery Point Objective
SRV	State Register of Voters
SRP	State Register of Population
RTO	Recovery Time Objective
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SAST	Static Application Security Testing
SBOM	Software Bill of Materials
SDK	Software Development Kit
DBMS	Database Management System
SIEM	Security Information and Event Management
SAISE or SAIS “Elections”	State Automated Information System "Elections"
SAISE Admin	SAISE Administrative Module
SLA	Service Level Agreement
SOAP	Simple Object Access Protocol
SPOF	Single Point of Failure
SQL	Structured Query Language
SSH	Secure Shell

Abbreviation	Full name
SSL/TLS	Secure Sockets Layer / Transport Layer Security
SSO	Single Sign-On
STISC	Information Technology and Cyber Security Service
TDD	Technical Design Document
ICT	Information and Communications Technology
ToR	Terms of Reference
ToT	Training of Trainers
UAT	User Acceptance Testing
ATU	Administrative-Territorial Unit
UC	Use Case
UI	User Interface
UNDP	United Nations Development Programme
URL	Uniform Resource Locator
UX	User Experience
VPN	Virtual Private Network
WBS	Work Breakdown Structure
WCAG	Web Content Accessibility Guidelines
WFS	Web Feature Service
WMS	Web Map Service
WMTS	Web Map Tile Service
WSO2	Web Services Oxygen
XLSX	Excel Open XML Spreadsheet
XML	eXtensible Markup Language
XSS	Cross-Site Scripting

3. Definitions

Acceptance (UAT) - The process through which CEC and end-users validate that the SRV meets the requirements in the ToR before Go-Live. It concludes with the acceptance document being signed by the Beneficiary.

Voter — a citizen of the Republic of Moldova who has reached 18 years of age and has the right to vote under the Electoral Code. Each voter is registered in the SRV with a unique IDNP and is assigned to a polling station according to their domicile address or declaration of residence.

Assignment — the process through which a voter is assigned to a particular polling station. Assignment is done automatically according to the domicile address from the SRP, manually by the registrar or on the basis of a declaration of residence. Once assigned, the voter casts their ballot at the respective polling station on election day.

Authentication — the process of verifying a user's identity. In the SRV, authentication is performed via MPass for citizens and civil servants.

Authorisation — the assignment of specific rights to a user already authenticated according to their role.

Backlog — the prioritised list of functionalities and requirements to be implemented under the project. It is prepared after the initial business analysis and updated during each sprint.

Technology database — a consolidated repository comprising all electoral data from SAISE and other CEC subsystems. It is the main source from which the SRV (current version) imports data about voters, polling stations and previous elections.

Backup — a copy of SRV data and configurations, stored separately from the operational system, used for data recovery in case of incident or disaster.

Beneficiary — the Central Electoral Commission of the Republic of Moldova, the body that procures and uses the SRV. It represents the public interest within the project.

DEC — District Electoral Council. A temporary electoral body established for each election, responsible for organising the election within the constituency. DEC users have read-only access to the data in their own constituency in the SRV.

Constituency — a territorial unit where elections are organised and votes are counted. DECs administer the electoral process at constituency level. In the SRV, the constituency defines the territorial access boundary for the CEC-DEC View role.

Cluster — a group of servers that operate together as a single logical unit, ensuring continuous availability and distributing load among components.

Conflict (data) — a situation where the same voter has different data in different sources. Conflicts must be checked and resolved either manually or via automated rules.

Service account — a system account used for automated processes (nightly import from the SRP, export of rolls to SAISE, synchronisations). It is not used by people, only by applications. It authenticates via digital certificates and has extended event logging.

Container (Docker) — a portable software unit that bundles an SRV component with all its dependencies. It enables identical execution in any environment (development, testing, production) and forms the basis of the SRV microservices architecture.

Declaration of residence — an official document by which a voter declares they temporarily live in a locality other than their permanent domicile. Based on this declaration, the person may vote at the polling station in the locality where they actually reside, not at the one of their domicile.

Depersonalisation — masking of personal data for unauthorised users.

Domicile — a person's permanent residence, officially recorded in the identity card and in the SRP. It is the primary basis for assignment to a polling station.

Dual control — a security principle whereby critical actions require two people with different roles: one executes, the other authorises.

ETL (Extract, Transform, Load) — the technical process that extracts data from external sources (SRP, SAISE), transforms them according to mapping and validation rules, and loads them into the SRV. It underpins periodic imports and the initial migration of data.

Failover — the automatic switch to the standby component when the primary component becomes unavailable, with no service interruption for users.

Contractor — the contracted company that designs, develops, implements and maintains the SRV under this ToR.

Go-Live — the moment the SRV is officially put into operation in the production environment, following the completion of acceptance tests and the CEC's approval. It marks the start of the warranty period.

IDNP — a unique 13-digit identifier assigned to every citizen of the Republic of Moldova, used as the primary key for identifying voters in the SRV.

Interoperability — the SRV's ability to communicate and exchange data with other systems (SRP, SAISE, MConnect) using common standards and protocols, without manual intervention.

Event logging — the automatic, permanent recording of all important events in the system: who authenticated, who changed which data, when, from where (IP, device), and with what outcome. The logs cannot be modified or deleted by users.

Electoral rolls — official documents listing all voters assigned to each polling station for a given election. The SRV generates these rolls and exports them to SAISE in an agreed format (PDF, CSV, XML) for use on election day.

Data Masking — partial display of personal data to protect confidentiality.

MConnect — the centralised government platform enabling public institutions in Moldova to exchange data securely. It provides a semantic catalogue (common definitions), secure channels and centralised event logging.

Environment (development / testing / production environment) - separate instances of the SRV for different purposes: development (work-in-progress code), testing (functional validation), pre-production (full rehearsal before launch), production (the live system used by the CEC). The separation of environments is mandatory for security and quality.

Metadata - "Data about data" — additional information describing who created a piece of information, when, from which source and in what format. Essential for traceability.

MPass - The system for online authentication of citizens using an electronic identity card, the digital ID on their phone, or username/password credentials. Managed by the Ministry of Information Technology.

Need-to-Know — the principle whereby each user sees only the data strictly necessary for their work. A Registrar in Orhei cannot see voters from Bălți.

Controlled list — a list of standard values used in the system for consistency: types of identity documents, localities from CUATM, types of election, voter statuses. It is centrally administered and versioned.

Normalisation — bringing data to a uniform format.

External QA — an independent company engaged by UNDP to monitor and control quality in the SRV implementation process. It participates in all project stages in an advisory role, without a unilateral right of veto; escalations are made to UNDP and the CEC.

RBAC (Role-Based Access Control) — a system in which rights are granted not to users directly, but to roles. A user is assigned one or more roles and automatically inherits all the permissions of those roles.

Registrar — a municipal employee who updates voter data in their area, registers declarations of residence and resolves local conflicts. The Registrar works only with data from the UAT for which they are responsible.

Resilience - the system's ability to continue operating (even in a limited mode) when problems occur: server outages, DDoS attacks, software errors. It includes automatic backup, redundant components and rapid recovery.

Rollback (controlled reversion) — returning data to a previous state while preserving the entire history. Unlike a technical rollback (DB transaction cancellation), in the SRV a new version is created that nullifies the effects of the previous version while keeping a complete record of what happened.

Election — the electoral event: parliamentary, presidential, local, regional elections, the national referendum or a local referendum. The SRV shall operate for all types of elections, with configurable rules for each.

Polling station — the physical place where people vote. Each polling station has a unique number, an address, a list of assigned voters and a maximum voter limit (usually 3,000).

Overseas polling station — a polling station set up outside the territory of the Republic of Moldova, attached to diplomatic missions. Diaspora voters are assigned to these stations based on declarations of residence submitted online.

SAISE — the CEC's information system for the electoral process. The SRV replaces the electoral rolls component of SAISE, while remaining integrated with it for data export/import.

SAISE Admin — the SAISE module for managing CEC users. The SRV recognises accounts from SAISE Admin and can perform single sign-on (SSO).

Synchronisation — the automatic update of SRV data with information from external sources, especially the SRP. It may be scheduled (for example, every night at 02:00) or performed on request.

SLA (Service Level Agreement) — a contractual agreement that defines the minimum service levels guaranteed by the Contractor: system availability, response times, and incident resolution times by severity category.

Sprint — a two-week development iteration in the Agile methodology ending with the delivery of demonstrable functionality. The SRV is developed through a succession of sprints, each with a backlog, a demo and a retrospective.

State (data) — the central concept in the SRV. A "state" is a time-fixed snapshot of a set of data, with a unique ID. It allows viewing data at a given moment, comparing differences between states and reverting to a previous state.

Voter status – the category of the voter: normal, military, detainee, institutionalised (hospital/care home), deceased, deprived of the right to vote (court order).

Threshold — a limit value configured to trigger an automatic action.

Timeout – the maximum waiting time before an automatic action is triggered.

Traceability – the ability to track the complete history of any data or action: who performed it, the precise time, what was changed (old value → new value), why (reason), and from where (IP, device).

ATU (Administrative-Territorial Unit) — administrative level: municipalities (Chișinău, Bălți), ATU Găgăuzia, districts, towns, communes, villages. Used to restrict Registrars' access strictly to their area of responsibility.

Validation — automatic verification that the entered data are correct and comply with the system rules (format, allowed values, referential integrity constraints).

Versioning – keeping every successive version of a piece of information. Unlike backup (a full copy of the system), versioning allows you to view the evolution of each individual record over time.

Workflow — a sequence of defined steps with clear roles and transition conditions between states. In the SRV, workflows govern processes that require approval or multi-party verification, such as data changes with dual control or conflict resolution.

4. Applicable legal and regulatory framework

The processes of creating, implementing, using and operating the State Register of Voters (SRV) must comply with the legal acts in force applicable to the electoral field and ICT (including cyber security, data protection, interoperability, state registers and common government services).

1. Electoral Code of the Republic of Moldova No. 325 of 08.12.2022, Official Gazette (published on 23.12.2022).
2. Law No. 101 of 15.05.2008 on the Concept of the State Automated Information System "Elections", Official Gazette Nos. 117–119, Article 457 (04.07.2008).
3. Law No. 48 of 30.03.2023 on Cyber Security, Official Gazette (published on 28.04.2023).
4. Government Decision No. 562 of 03.09.2025 on the Fulfilment of Cyber Security Obligations by Service Providers in Critical Sectors.
5. Law No. 133 of 08.07.2011 on the Protection of Personal Data, Official Gazette (published in 2011).
6. Law No. 195 of 25.07.2024 on the Protection of Personal Data (the new law) – published in Official Gazette Nos. 367–369 (2024) and enters into force on 23.08.2026; until then, the provisions of Law No. 133/2011 are applied.
7. Law No. 124 of 06.10.2022 on Electronic Identification and Trust Services, Official Gazette (published on 10.06.2022).
8. Law No. 142 of 19.07.2018 on Data Exchange and Interoperability, Official Gazette (published on 17.08.2018).
9. Government Decision No. 211 of 14.03.2019 on the Interoperability Platform (MConnect), Official Gazette (published on 29.03.2019).
10. Government Decision No. 1090 of 31.12.2013 on the Government Authentication and Access Control Service (MPass).
11. Government Decision No. 405 of 02.06.2014 on the Integrated Government Electronic Signature Service (MSign).
12. Government Decision No. 128 of 20.02.2014 on the Common Government Technology Platform (MCloud).
13. Government Decision No. 152/2021 on the Concept of the Governmental Delivery Service (MDelivery) – if relevant to processes involving the delivery of results to citizens/institutions.
14. Law No. 305 of 26.12.2012 on the Re-use of Public Sector Information;
15. Law No. 91 of 29.05.2014 on the Electronic Signature and the Electronic Document;
16. Government Decision No. 330 of 04.05.2010 on the Creation and Administration of the Single Government Portal for Public Services;
17. Government Decision No. 5 of 10.01.2024 on the EVO Integrated Government Application for Electronic Services.
18. Law No. 467 of 21.11.2003 on Informatization and State Information Resources, Official Gazette (published on 01.01.2004).
19. Law No. 71-XVI of 22.03.2007 on Registers, Official Gazette (published on 25.05.2007).
20. Order of the Minister of Information Development No. 78/2006 Approving the Technical Regulation "Software Life Cycle Processes" RT 38370656-002:2006.
21. Government Decision No. 708 of 28.08.2014 on the Government Electronic Event Logging Service (MLog);
22. Government Decision No. 376 of 10.06.2020 approving the Concept of the Government e-Notification Service (MNotify) and the Regulation on the Operation and Use of the Government E-Notification Service (MNotify);
23. Government Decision No. 677 of 08.10.2025 on Strengthening Access to Electronic Public Services within the Integrated EVO Government Portal used for the Provision of Electronic Public Services and Approving the Measures Necessary to Implement the Unified Design Model.
24. CEC Decision No. 1140 of 28.07.2023 approving the Regulation on the State Register of Voters (repealing certain previous related acts).
25. The Central Electoral Commission's internal regulations relating to processes and activities subject to the SRV & SAISE (to be presented to the selected Contractor as required).

Standards and best practices in the ICT field:

1. SM ISO/IEC/IEEE 15288: 2024 "Systems and software engineering. System life cycle processes".
2. Standard SM ISO/IEC/IEEE 14764:2022 - Software engineering. Software life cycle processes. Maintenance;

3. Standard SM EN ISO/IEC 27001:2017 - Information technology. Security techniques. Information security management systems. Requirements;
4. Standard SM EN ISO/IEC 27002:2017 - Information technology. Security techniques. Code of good practice for information security management;
5. Standard SM ISO/IEC 15408-1:2022 — Information security, cybersecurity and personal data protection. Evaluation criteria for IT security. Part 1: Introduction and general model;
6. Standard SM ISO/IEC 15408-2:2022 — Information security, cybersecurity and personal data protection. Evaluation criteria for IT security. Part 2: Functional security components;
7. Standard SM ISO/IEC 15408-3:2022 — Information security, cybersecurity and personal data protection. Evaluation criteria for IT security. Part 3: Security assurance components;
8. Level AA user interface requirements of the 'Web Content Accessibility Guidelines 2.1', https://www.w3.org/TR/WCAG21/;
9. World Wide Web Consortium (W3C) recommendations (http://www.w3c.org) on the quality of web page content, accurate display of information using widely used web browsers, and compatibility with various computing platforms;
10. OWASP Top 10 Guide for web application security;
11. W3C recommendations (http://validator.w3.org) regarding testing web pages. All web pages generated by the SRV shall be tested in accordance with these recommendations;
12. Resource egov4dev — the official documentation library for developers working with the EGA ecosystem, providing guidance on integrating government platforms and services, using the common development technology stack, and adhering to the established architectural principles.

5. Scope and objective of the procurement

The subject of the procurement is the development and implementation of an information system intended for managing the State Register of Voters (SRV), in line with the provisions of the applicable legal framework. The System shall allow the establishment, updating, eligibility verification, generation of electoral rolls, as well as interconnection with relevant registers and controlled access by voters to their own data. It will support the activity of the Central Electoral Commission and the authorities involved, ensuring the integrity, transparency and efficiency of electoral processes.

Through this procurement process, UNDP as part of the capacity building activities delivered to the CEC, with the support of development partners and the participation of independent experts and other state institutions and authorities, is procuring complex services for the development, implementation and post-implementation maintenance of the application suite, supporting software components and the services required for the SRV operation under the conditions set by the legal framework, internal regulations and the requirements for related areas (information security, personal data protection, record-keeping, interoperability, etc.).

The System shall ensure the integration of current internal and external information sources, provide secure and efficient tools for managing data from different sources, formats and with varying levels of accuracy, allow the CEC to identify inconsistencies and divergences/conflicts, and provide the tools necessary for the preparation of the data that are the subject of SRV record-keeping (in accordance with legal and security requirements).

Even though at present several data sources may not be available for integration and the real-time (online) provision of data, the System shall be flexible, scalable and adaptable for the subsequent integration of other data sources as they become available and as the technical conditions for integration/interoperability allow.

The SRV is being implemented to replace the current version of the IS 'State Register of Voters', while preserving the core functions and the functional and design concept. When implementing the new SRV, data from the old system must be imported, with cleansing and correction carried out as required. Currently, the data in the TechDB (which also includes the DB used for the current version of the SRV) contain a number of nonconformities and inconsistencies that must be handled individually during the import process.

Notable problems and deficiencies in the current SRV’s data and operation include data conflicts and duplications, and problems with defining polling stations, particularly for localities without defined streets, or where streets cross several localities, etc.

6. CEC Technology Architecture and Data

Data architecture

From a data architecture perspective, the CEC is a central node that aggregates, validates, consolidates and redistributes electoral data to and from polling stations/offices, as well as external actors.

The data are segmented through specialised subsystems/functional blocks, each with its own databases, rules and life cycles. At the centre, there is the administration and configuration component (SAISE Admin) which, besides the administration and access management for subsystems, also provides digital support for the business functions tied to election preparation (election management, generation of the database for election day, returning data on the vote, as well as notification management, etc.).

Internal communication is carried out through data exchanges between modules with functional dependencies via APIs provided by SAISE Admin, as well as other subsystems, as required.

The CEC ecosystem interacts with various state institutions for data exchange, validations and confirmations, consumed in different formats (e.g. automated, unstructured data or paper-based data) including identity registers and public services (via PSA/EGA), border services (MIA), the Ministry of Justice, courts, penitentiary institutions, control and audit (the Court of Accounts), as well as constitutional actors (Parliament, the Constitutional Court) for reporting/confirmation purposes.

As already specified, the architecture is mixed: there are structured digital (automated) flows, unstructured digital flows (semi-automated, file exchanges, electronic documents, notifications), and traditional unstructured flows (paper, offline processes).

The RSV shall be designed to enable the granular integration of external data sources, as they become available and meet the required standards for quality, content, and timeliness. For the purpose of establishing a reference framework for external data to be obtained either automatically (via MConnect) or through other available methods, Annex No. 1 – Data Sets is provided. The system must be capable of operating as designed, regardless of the method used for data acquisition or input.

Application architecture

The CEC ICT architecture is built on a centralised model of access governance, interoperability and operational control, with SAISE Admin as the single point of access and orchestration for most applications that digitally support the electoral processes.

Besides SAISE Admin, the State Automated Information System “Elections” includes a set of applications covering distinct electoral processes: management of rolls and subscriptions, observers management, operational rotation/organisation, documentation, ballot papers, execution on E-Day, financial control, etc.

SAISE Admin functions as the central administration element, ensuring user management, authentication, authorisation and correlation of access rights for the integrated applications. Applications enrolled in SAISE Admin consume centralised security APIs, used for authenticating users and establishing their rights on the basis of an RBAC (Role-Based Access Control) access model. For each application, the roles and sets of permitted actions (transactions) are explicitly defined, removing implicit access and reducing the attack surface.

Additionally, SAISE Admin provides the enrolled applications with APIs for:

- Recording audit events. Audit events generated at each application level are recorded in SAISE Admin;
- Management of common controlled lists.
- Notification management.
- Provision of a list of reports.

At the functional level, the architecture is structured into multiple layers:

- *Core applications layer (electoral core)*

Includes applications such as ISS Subscription lists, Electronic subscription lists, ISS Observers, ISS Rotation, ISS Documentation, ISS Ballot papers, ISS E-Day, ISS Financial control, ISS Register of electoral officials and ISS Centralisation of the voting results. These applications manage electoral cycle processes and are integrated with SAISE Admin.

- *Layer of public and informational applications*

Includes applications and portals such as rezultate.cec.md, votează.md, alegător.md, diaspora.cec.md, vpc.cec.md, cec.md, votcorespondența.cec.md, and cece.cec.md. Their focus is on transparency, public information and access to aggregated data, with controlled feeds from internal applications.

- *Data and analytics layer*

CEC uses the Microsoft SQL Report Service to produce shared-use reports by consolidating operational data for analysis, reporting and decision support, without directly interfering with critical transactional systems. These reports are registered in SAISE Admin and are accessible to applications through the specialised API provided by SAISE Admin.
Reports defined in MS SQL Report Service are cross-application. There are reports that extract data from DBs belonging to different applications. The logical integrity constraints defined at application level are not automatically propagated to the reports. Integrity requirements are defined separately for each report.
CEC analyses and plans the implementation of a DWH.

- *Integration layer*

It is represented by components such as the CEC interoperability bus (WS02 DSS), as well as limited interconnection with MCloud services. CEC integrates with external systems such as FPS (AIS FRS), AIS MF through controlled and standardised channels, mainly via the interoperability bus.
At present, interoperability between applications is achieved in three ways:

1. Sharing the database with the satellite application. Several applications have satellite applications, such as AIS SRV (current version), ISS e-Day, ISS Observers, ISS Rotation, etc. Satellite applications are typically widgets and portlets. Several widget-type applications are web implementations intended to embed information from ISS Rotation into web pages. Portlet applications are created to run at server level. Both are presented as modules of their parent applications. In the application diagram, they appear as components of the parent application, linked by an aggregation relationship.
2. Use of the API provided by the donor application. This is the most common mode of interaction between CEC applications, including with external ones. The most telling example is the interaction between SAISE Admin and the integrated applications.
3. Use of the interoperability bus. The CEC uses the WSO2 DSS platform solution as an interoperability bus. It is used by the ISS Financial Control application as well as by SAISE Admin.

Most of the applications used by the CEC were supplied by two developers. As a result, the architecture, the technologies used, and the design are largely similar.

Technology architecture and the implementation environment

The institution has its own suitably equipped data centre; however, maintenance and the refurbishment of certain components are required. It is located at the central office, in a dedicated area.
The ICT network architecture is designed on a hierarchical, segmented and controlled model. Its main objective is to support CEC's critical applications, ensure operational continuity, and limit security risks by separating functional zones.
The CEC operates a server infrastructure based on virtualization using Hyper-V. Most internal servers are virtualized and run Windows Server operating systems. Current Information Systems are developed using Windows-compatible technologies, with MS SQL predominantly used as the database management system.
The CEC will provide the necessary technical resources for hosting RSV components and support services within its own infrastructure. Additionally, CEC has access to a shared Government Git platform, which may be used for workflow integration, should this be deemed feasible.

The SRV shall be developed and deployed in a manner compatible with Moldova's government digital infrastructure and the technical standards applied across state information systems. The minimum required technology profile for the proposed solution is as follows:

- Containerisation: The solution shall be packaged as OCI-compliant container images (Docker), using minimal Linux base images optimised for the container environment. All components must be capable of running in virtualised environments without restrictions.
- Orchestration: Container orchestration shall be implemented using Kubernetes (K8s), deployable over the Government Cloud (MCloud/OpenStack) infrastructure.
- Operating system: Red Hat Enterprise Linux-compatible distributions (Rocky Linux or AlmaLinux

preferred for their binary compatibility with RHEL and absence of licensing costs) or Debian-family distributions (Ubuntu LTS, latest long-term support release). Rocky Linux is the preferred choice.

- Database: PostgreSQL is the preferred relational database management system. MS SQL Server 2022, configured to run in Linux containers, is an acceptable alternative where technically justified.
- Backend framework: .NET 10 (cross-platform) with Entity Framework Core as the ORM layer.
- Frontend: A modern JavaScript framework (Angular, React, or Vue) supporting ECMAScript 2025 (ES16) or higher, targeting standards-compliant browsers without proprietary plugins. The frontend shall be implemented in conformity with the Unified Design Model (MUD) established under Government Decision No. 677 of 08.10.2025. Public-facing portals shall support Server-Side Rendering (SSR). All interfaces shall comply with WCAG accessibility standards. UI/UX design shall be developed using Figma and delivered with full design documentation.
- API design: All public and interoperability APIs shall follow a spec-first approach, documented in OpenAPI 3.1 format.
- Messaging and streaming: RabbitMQ or Apache Kafka for asynchronous communication between microservices.
- Object storage: MinIO or equivalent S3-compatible object storage.
- Search and analytics: OpenSearch for full-text search; ClickHouse for columnar analytics where applicable.
- Source control and CI/CD: Git-based version control (Gitea or self-hosted GitLab CE), with an automated CI/CD pipeline incorporating static application security testing (SAST) and secret detection at each build stage.

All technologies proposed must have active long-term support (LTS or equivalent) for a minimum of three years from the date of contract signature, and must contain no end-of-life components. Where a Contractor proposes an alternative to any of the above, the deviation must be technically justified in the proposal, with an explicit explanation of how long-term maintainability and CEC ownership of the solution are preserved.

7. Stakeholders, participants in the process

Stakeholders

Within this project, the following stakeholders are defined:

#	Name	Details
1	**Funder (UNDP)**	The UNDP "Strengthening Democratic Resilience in Moldova" (EDMITE III) Project. It shall ensure the project funding and will monitor development, implementation, and maintenance/post-implementation support activities.
2	**Beneficiary (CEC)**	Central Electoral Commission (CEC) – public authority established to implement electoral policy and to ensure the proper organisation and conduct of elections. The CEC's mission is to create optimal conditions for the citizens of the Republic of Moldova to exercise, without hindrance, their constitutional right to vote and to be elected in free and fair elections. CEC is the owner of the SRV and the primary beneficiary of this project's results. The CEC ensures the administration and updating of the SRV.
3	**QA**	A company operating under a service contract with UNDP, which participated in drafting the Terms of Reference and has the role of supervising and monitoring the SRV implementation process.
4	**PSA**	The Public Services Agency as an information provider, via the State Population Register, concerning persons entitled to vote (date of birth, surname, forename, IDNP, etc.).
5	**STISC**	The State Enterprise "Information Technology and Cyber Security Service" as the entity administering the MCloud solution that delivers platform services implemented under the SRV, being also responsible for hosting the servers running SAISE and its components.
6	**EGOV**	The e-Governance Agency as the body mandated to develop and implement the e-Transformation policy, the MCloud solution and the MConnect interoperability framework used to enable the SRV's interaction with external information systems (the State Register of Persons) and platform services (MPass, MSign, MLog, etc.).

Participants in the implementation process

Pursuant to the SRV-related legislation in force and based on official mandates, alongside the stakeholders, the following participants in the SRV formation process are identified.

#	Name	Details
1	**MoJ**	The Ministry of Justice and its subordinate institutions: - National Probation Inspectorate - Agency for Digitalisation in Justice and Court Administration They provide information required to build the SRV, such as: - information on persons sentenced to imprisonment (deprivation of liberty) by a final court judgment; - information on persons with unspent criminal convictions for offences committed intentionally; - information on persons deprived, by a final court judgment, of the right to hold public office or positions of public dignity.
2	**NUB**	The National Union of Bailiffs, responsible for presenting information on persons convicted of intentional offences and sentenced to a criminal fine, but who have not fulfilled their payment obligation.
3	**MLSP**	The Ministry of Labour and Social Protection, which is responsible for providing information about persons with disabilities

#	Name	Details
4	**MIA**	The Ministry of Internal Affairs, through MIA's Information Technology Service, which shall provide information on the existence and status of criminal investigation case files opened against the persons checked.
5	**MER**	The Ministry of Education and Research holds the following information: information on student status within educational institutions of the Republic of Moldova, required to admit the voter to vote according to the educational institution's address.
6	**NPA**	The National Penitentiary Administration, which holds information on detainees, their number in each penitentiary, and how many are not citizens of the Republic of Moldova or are not entitled to vote.
7	**PI "Cadastru"**	The Public Institution Cadastre of Immovable Property – the holder of the State Register of Administrative-Territorial Units and Addresses, which includes the Classifier of the Administrative-Territorial Units of the Republic of Moldova (CUATM).

8. **Business Roles (system roles)**

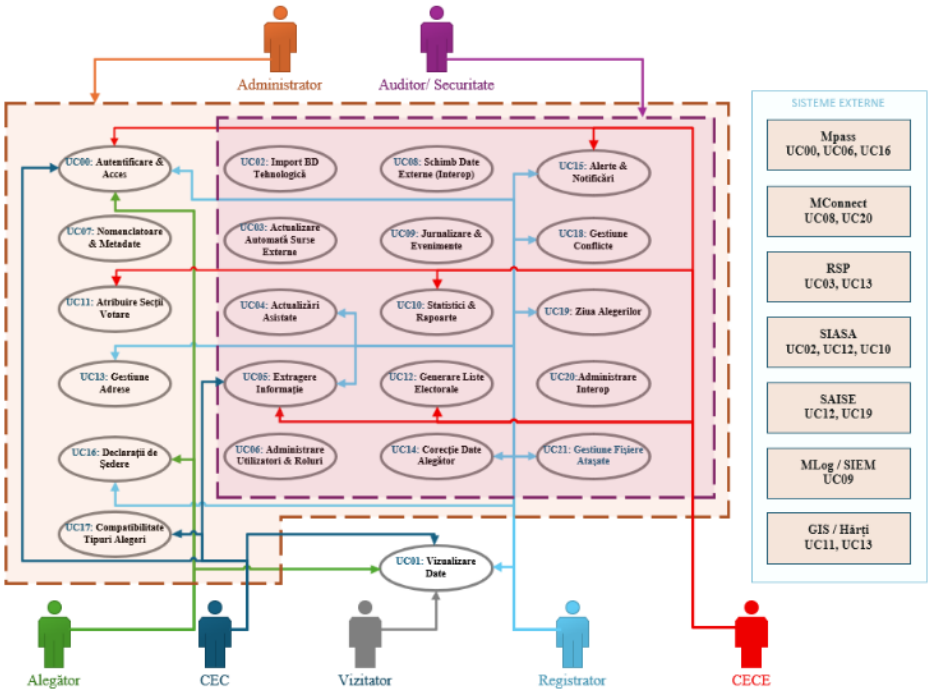

Figure 8.1. Roles vs use case diagram

The human roles that interact with the SRV are presented in Figure 8.1. Within the application, seven categories of human actors will interact, together with the information systems integrated with the SRV. The functions and access rights for each role or user group shall be configurable, including for aspects not explicitly described in this document, which will be further defined, required, or agreed upon during implementation or in the maintenance phase

1. **Visitor** – unauthenticated users who access the SRV through the public web interface, without holding an account in the system. They will have access to the following functionalities:
    - checking the existence of a voter in the SRV using the IDNP (yes/no answer)
    - viewing depersonalised and masked data (initials, date-of-birth reference, and the number and address of the polling station);
    - receiving standardised system messages ("does not exist", "cannot be displayed");
    - access is subject to anti-abuse mechanisms (CAPTCHA, rate limiting, temporary blocking after a configured number of queries).
2. **Voter** – citizens of the Republic of Moldova authenticated via MPass who access the SRV to check their own data and exercise the rights provided by law. They will have access to the following functionalities:
    - viewing the complete personal data from the SRV (surname, given name, domicile, polling station, list number, etc.);
    - checking their own status on the electoral rolls;
    - registering a declaration of residence for the active election, in line with the established deadlines;
    - registration of the voting rights certificate;
    - viewing the assigned polling station and its address;
    - receiving notifications on relevant changes (if the EVO service is available).
    - all data and functionalities available to the **"Voter"** role will be available both through direct access to the SRV and through the EVO government portal.
3. **Registrar** – CEC or municipal officials authorised to handle voter data within the administrative-territorial unit of their responsibility. access is strictly limited by territory to the ATU assigned to the account. They will have access to the following functionalities:

- searching and viewing voter data from their own ATU, in line with the associated rights;
- updating and correcting voter data on the basis of supporting documents, with mandatory justification;
- changing the voter's status (deceased, declared deceased, institutionalised, etc.) with the supporting document attached;
- registering and managing declarations of residence for voters within their area of responsibility;
- handling local data conflicts (addresses, status, polling station assignment);
- assigning and modifying the polling station for voters in the ATU;
- all manual interventions require the application of the principle of double-checking and authorisation (dual control);
- receiving notifications and alerts related to activities within their own ATU.

4. **CEC – View** – denotes authorised users of the Central Electoral Commission who interact with the SRV to check data and generate reports at national level, without the right to modify data. They will have access to the following functionalities:
    - searching and viewing voters' data at the national level, in line with the associated rights;
    - generating and exporting aggregated statistical reports (by country, district, municipality, polling station);
    - checking the electoral rolls for any election registered in the system;
    - visualising polling stations and the distribution of voters;
    - use of the operational dashboard;
    - receiving notifications.
5. **CEC – DEC – View** – represents authorised users of the District Electoral Councils who interact with the SRV to check data from their own constituency, without any right to modify data. Access is limited to the assigned constituency. They will have access to the following functionalities:
    - searching and viewing voter data from their own constituency, in line with associated rights;
    - generating and exporting local reports (polling station, locality, constituency);
    - checking the constituency's electoral rolls;
    - using the operational dashboard for their own constituency;
    - receiving notifications.
6. **Audit / Security** – represents authorised CEC users responsible for monitoring, control and auditing of the SRV's activity. They will have access to the following functionalities:
    - viewing and exporting security and audit logs (read-only);
    - mandatory authorisation for changes to roles, groups and security parameters (dual control);
    - generating audit and compliance reports;
    - monitoring security events and system alerts;
    - configuring the categories of events sent to MLog and SIEM;
    - access to encrypted logs is provided exclusively via the built-in system account.
7. **Administrator and Data Administrator** – a human actor responsible for ensuring the SRV operates under optimal conditions. This category of actors has access to the following functionalities:
    - unrestricted use of the system's functionalities, except for modifying log files;
    - management of the SRV's controlled lists, classifiers and metadata;
    - management of users, roles and access rights through the SRV's RBAC mechanisms;
    - configuring the SRV's resources, roles, transactions and workflows;
    - configuring reports and templates for report generation or data export.
    - administration of integrations with external information systems (SRP, SAISE, MConnect, MPass, MSign, MLog, MNotify, etc.);
    - monitoring the SRV's operation;
    - launching, stopping and suspending SRV functionalities (where authorised);
    - The accounts in this category shall be customised.
    - Certain categories of functions and rights may be granted differently from one account to another.

- **They may not modify credentials, the authentication method, or the rights of other privileged accounts. They may not create, delete, or disable administrative accounts.**

8. **SuperAdministrator** – a reserve, "break glass" administrative account with full rights over all functions and operations, without exception. The access password shall have advanced length and complexity requirements and shall not expire. This account may be used only with authentication via username and password. Its purpose is to allow intervention in emergencies, including creating a new administrative account or changing credentials for administrative accounts.

Note: *User groups, granular rights, and authorisation flows will be defined in detail during the preliminary analysis phase.*

9. Functional Model

Use cases and functional requirements

General functional requirements that apply to the entire system. These requirements may be supplemented or detailed by the specific requirements in the other categories (cross-cutting FR – apply across the entire SRV).

Table 9.G. FR-GEN – General requirements

Identifier	Mandatory status	Description of requirement
FR-GEN.01	**M**	The SRV shall implement role-based access control (RBAC) and the "need-to-know" principle for data and actions.
FR-GEN.02	**M**	The SRV shall log critical actions (authentication, data changes, export, conflicts, jobs, interop), including user, time, result, and source. **Note:** this requirement will be complemented (aggregated) with the specific logging requirements (relating to logs) in the other chapters; only the generic requirements are indicated here.
FR-GEN.03	**M**	The SRV shall ensure the integrity of logs (not modifiable by users) and allow access only to authorised roles.
FR-GEN.04	**M**	The SRV shall validate input/received data (format, mandatory fields, consistency and controlled lists).
FR-GEN.05	**M**	The RSV shall maintain full traceability of all changes and all "states" of data and documents (who/what/when/why/source/method of acquisition), with each state assigned a unique identifier.
FR-GEN.06	**M**	The SRV shall apply anti-abuse and anti-exfiltration measures for queries/exports (rate limiting/throttling, volume limits, logging).
FR-GEN.07	**M**	The SRV shall manage notifications/alerts for critical errors, unusual volumes, and security events (in line with configurable thresholds).
FR-GEN.08	**M**	The SRV shall manage official controlled lists and mapping tables (normalisation), with controlled import/export and versioning.
FR-GEN.09	**M**	The SRV shall support standard exports (PDF/CSV/JSON/XLSX/HTML where applicable) with preview and audit (who/when/criteria/volume/format).
FR-GEN.10	**M**	The SRV shall manage integration with external systems through secure channels and an approved authentication/authorisation mechanism (keys/certificates/technical MPass, etc.).
FR-GEN.11	**M**	The SRV shall support operational monitoring (process status, errors, timings, usage statistics) for authorised roles.
FR-GEN.12	**D**	The SRV shall allow configuring parameters (thresholds, validation rules, execution windows) without code changes, where supported by the architecture.
FR-GEN.13	**M**	The SRV shall support a multilingual interface (RO/RU/EN) for the public area, as well as for error and warning messages. Names and displayed text shall be automatically synchronised with the language selected by the user in the respective menu.
FR-GEN.14	**M**	Texts displayed on graphical elements, buttons, error messages, system messages and pop-ups shall match the language used for the graphical display.
FR-GEN.15	**D**	The System shall block the use of data copy-to-clipboard functions for all user accounts, except for administrative functions.
FR-GEN.16	**M**	The System shall allow integration with GIS-type systems based on OGC (Open Geospatial Consortium) standards. At least the following standards shall be supported: - WMS (Web Map Service) - WFS (Web Feature Service) - WMTS (Web Map Tile Service) - OGC API – Features/Maps

Identifier	Mandatory status	Description of requirement
FR-GEN.17	**M**	The System shall have dedicated menus for localisation based on text entered directly or through providing structured files.
FR-GEN.18	**M**	The System shall ensure integration with the Citizen's Cabinet through the government EVO service, using the MPass (Authentication and Access Control Service). Within the EVO personal cabinet, the citizen shall have the option to be redirected to their RSV account without the need for repeated authentication.
FR-GEN.19	**M**	For voters (authenticated citizens), the System shall provide a personal cabinet function with available detailed data about the person concerned (surname, given name, domicile address, date of birth, polling station number and address, electoral roll number, and other data as specified below). **Note:** the exact necessary information to be displayed will be defined/agreed at the SRV implementation stage, based on the internal and external data available.
FR-GEN.20	**M**	All external data flows shall be carried out through MConnect, except in cases where this is not technically feasible.
FR-GEN.21	**M**	All internal integrations shall be implemented through the internal interoperability platform based on DSS WSO2. The Contractor shall ensure comprehensive documentation for all integrations and data flows.
FR-GEN.22	**M**	The system shall use the MSign platform service as the mechanism for applying and validating electronic signatures. The service shall be available by default for all cases and scenarios involving the signing or verification of document signatures.

UC01: Accessing the SRV

UC01 is the SRV capability to provide users with access matching their roles/rights, and to allow management of the authentication process.

Table 9.1. Functional requirements for use case UC01

Identifier	Mandatory status	Description of requirement
FR 01.01	**M**	The SRV shall provide access to system functionalities and data according to the user type and their access rights.
FR 01.02	**M**	Authorised users of the SRV authenticate through MPass service (intended for authentication via electronic or mobile signature), with the option to access the SRV from the citizen's personal cabinet (EVO.GOV.MD).
FR 01.03	**M**	The SRV shall provide authentication tools based on alternative methods if MPass is unavailable.
FR 01.04	**M**	The SRV shall provide configuration options for authentication mode for accounts or user groups, without using MPass.
FR 01.05	**M**	The SRV shall allow anonymous access in line with the access level set for unauthenticated users.
FR 01.06	**M**	At each authentication, the user will be shown information about: - The exact date and time of the last authentication - Information about the device used to access the system - The duration of the work session - The location and/or IP address for the access
FR 01.07	**M**	The System shall manage authorised users' sessions and allow automatic session termination after a period of inactivity (it shall be set and be adjustable for each user group).
FR 01.08	**M**	The System shall prevent parallel sessions for the same authorised user account (different locations, different browsers, etc.).

Identifier	Mandatory status	Description of requirement
FR 01.09	**M**	The System shall prevent simultaneous sessions from the same device for different accounts.
FR 01.10	**M**	The System shall record all actions related to authorised users' access (successful/failed authentication, credential changes, etc.), including details of the device used, IP address, etc.
FR 01.11	**M**	For users with roles entailing access to personal data, at each authentication, before access is actually granted, the system shall display a warning message and an acceptance prompt for the requirements/rules on accessing personal data.
FR 01.12	**M**	The System shall send alerts to administrators in the event of multiple failed access attempts (brute-force) as follows: 1. SRV application-level alerts 2. Email alerts, according to an editable list.

UC02: Import and validation of data from the TechDB

The technology database is a data repository containing information from the State Automated Information System "Elections" and other systems and subsystems. Data shall be updated with information from the TechDB for the fields defined/set at the implementation stage. The use case aims to ensure the receipt, validation, normalisation, and integration of data from the TechDB into the SRV, with conflict management and preserving full traceability.

Table 9.2. Functional requirements for use case UC02

Identifier	Mandatory status	Description of requirement
FR 02.01	**M**	The SRV shall be based on data from the TechDB, ensuring the full import of current data and structures. The imported data shall be documented and used by the Contractor for the operation of the SRV. The SRV shall receive and process requests from the TechDB in line with the established workflow.
FR 02.02	**M**	The SRV shall validate and normalise the received data (schemas, mandatory fields, metadata, correspondence tables). SRV shall validate technically and logically data received from the TechDB (format, schema, mandatory fields, types, constraints, consistency with the SRV controlled lists) and shall normalise the data through mapping tables and standardisation rules so that external data are compatible with the SRV model and codes.
FR 02.03	**M**	The SRV shall perform admissibility checks (technical and business) and shall separate rejected items with stated reasons. - For all records and fields with discrepancies, the System shall allow selecting the action to take (actions will be determined depending on the type of conflict and data). - Data with conflicts or errors that have not been updated shall be flagged, and the System shall generate a detailed report required for cause analysis. - The System shall allow repeated imports of data for records where errors were returned or conflicts existed. - The administrator responsible for the import shall validate the final version of the data for import — thereby completing the import operation.
FR 02.04	**M**	The System shall provide the ability to select fields for update using graphical interfaces (UI).
FR 02.05	**M**	The System shall allow use of the data according to the recorded states for operation. Thus, the Administrator shall define the "state" (data version) that will be actually used "in production".
FR 02.06	**M**	The SRV shall allow viewing the differences (before/after) for each request.

Identifier	Mandatory status	Description of requirement
		The differences shall be exportable in the selected format (CSV, XLSX, XML/JSON, PDF).
FR 02.07	**M**	The SRV shall allow classification (filtering) of requests (enquiries): automatic / assisted / conflict / rejected / stopped, and by other relevant criteria.
FR 02.08	**D**	The SRV shall generate detailed reports for each processing operation (volume, accepted, rejected, conflicts, errors, etc.).
FR 02.09	**M**	The Contractor shall ensure the preservation of functionalities of other systems and components that use data from the current TechDB and need to be connected to the SRV, including the creation of APIs for integration with existing applications.

UC03: Automatic update and management of data from external sources

UC03 is the SRV capability to receive and process data from external sources, automatically applying updates deemed safe according to the configured rules. The System allows defining the fields and update parameters, semi-automatic import of unsafe data, and retention of all "states" with unique identifiers and full traceability.

Table 9.3. Functional requirements for use case UC03

Identifier	Mandatory status	Description of requirement
FR 03.01	**M**	The SRV shall automatically apply updates deemed safe from external sources (for example, SRP), in line with the configured rules. **Note:** external sources shall be integrated over time; the actual list and the data available from them shall be set at the implementation stage, depending on the capacity of institutions to provide data sets in line with the requirements for content, timeliness, and quality. For the purpose of defining these data sets and the related specific requirements, the Contractor shall use, as a reference, but not be limited to, the requirements set out in Annex No. 1 – SRV Data Sets.
FR 03.02	**M**	The list of safe data and data sources shall be configurable. The Administrator shall define the data deemed safe, which will be automatically taken from external sources, being regarded as current (baseline) data.
FR 03.03	**M**	The System shall allow importing data from external sources (other than those indicated in FR 03.01) without actually updating the data in the SRV (database). The system shall allow the integration of new internal and external data sources, replacing or complementing manual or semi-automated workflows, without the need to make changes to the codebase.
FR 03.04	**M**	The SRV shall use configurable rules for automating data updates, such as: - permitted fields, - thresholds/parameters: date, locality, age, etc., - types: changes or data categories, - others. Data not considered safe (see FR 03.01) shall be imported without updating the data. Such data shall be updated semi-automatically by the **data administrator.**
FR 03.05	**M**	The System shall provide the ability to select fields for update using graphical interfaces (UI).
FR 03.06	**M**	The System shall allow use of the data according to the recorded states for operation. Thus, the Administrator shall define the "state" (data version) that will be actually used "in production".
FR 03.07	**M**	The SRV shall allow viewing the differences (before/after) for each request. The differences shall be exportable in the selected format (CSV, XLSX, XML/JSON, PDF).

Identifier	Mandatory status	Description of requirement
FR 03.08	**M**	The SRV shall allow authorised roles to analyse automated runs (status, result, errors). To this end, a dashboard shall be displayed containing at least the following details in real time: - Percentage and number of records processed, and the total number. - Number of records where data were modified. - Number of records with errors. - Number of records requiring verification/intervention.
FR 03.09	**M**	The SRV shall generate summary (aggregated) reports per run (processed, rejected, conflicts, duration, errors). Reports may be exported in PDF and HTML, and saved or sent to the **data administrator's** email address.
FR 03.10	**M**	The SRV shall allow controlled reprocessing of a set of records, with traceability.
FR 03.11	**M**	The SRV shall allow temporary suspension of automations in case of risk/maintenance.
FR 03.12	**D**	The System shall allow a complete stop of the update process, with a full rollback to the pre-initiation state.
FR 03.13	**D**	The System shall enable a temporary pause and resumption of the update process.
FR 03.14	**M**	The System shall allow scheduling the launch of the update process. In such cases, the System shall send automatic email reminders according to a defined schedule, and application-level alerts.
FR 03.15	**M**	For any data/fields derived from information that can be entered/corrected manually (e.g. withdrawal of citizenship or of the right to vote, death, etc.), the System shall allow integration of external data sources through files or automatically (MConnect / API).
FR 03.16	**M**	The System shall allow defining mapping rules for important data from source data to fields in the SRV DB, without the need to modify the source code.
FR 03.17	**M**	External sources shall include other systems and CEC DBs/services that contain data or controlled lists that must be reused, without duplicating data.

UC04: Processing assisted updates

UC04 represents the system functionality/capability to perform customised updates from various sources, in order to handle conflicting or incomplete (outdated) data. This use case complements and continues UC02 and UC03. These use cases define the requirements for analysis, verification, cross-checking, and correction/update of data in substantiated cases (errors, the existence of supporting documents, outdated data in external sources, etc.). Additionally, the System shall allow targeted updates or corrections of data in line with certain preconditions (criteria).

Table 9.4. Functional requirements of Use Case UC04.

Identifier	Mandatory status	Description of requirement
FR 04.01	**M**	The SRV shall provide an interface to approve, reject or ignore assisted requests to update or correct data. In particular, these relate to persons declared deceased.
FR 04.02	**M**	The SRV shall provide registrars with the ability to change a voter's status: Deceased / Declared Deceased (as per the controlled list). When changing the status, the SRV shall require attachment of a death certificate (local or from abroad). The SRV shall provide a tool for recording attached documents, by including their type (preferably from controlled lists), number and date of issue, issuing authority, a brief description, and the attached document itself.
FR 04.03	**M**	The SRV shall allow batch processing for certain selected requests.

Identifier	Mandatory status	Description of requirement
FR 04.04	**M**	a) Each update, correction, deletion or other type of manual data intervention shall require dual verification and authorisation. Thus, each case shall be accepted for execution, upon acceptance of the preconditions, as follows: - Confirmation of verification. - Authorisation by a designated person (depending on the type of data). - Attachment of evidence and justification/description of the operation. b) The System shall generate logs for all such actions, detailing the actions of each party, the time, and the device used to perform them. c) If the process was stopped at any stage (e.g. no authorisation), all details of the initiated action shall be retained, with the DB data remaining unmodified/unaffected. d) If at any stage an error, omission, or any other reason for rejection is found, the process shall be restarted from the beginning for adjustment, while the previous instance is kept in its stopped state. Note: the persons included in the verification and authorisation workflows shall be specified by name during implementation.
FR 04.05	**M**	The SRV shall allow the data to be filtered/sorted/prioritised (by type, severity, locality, period, etc.) for updating/rectification.
FR 04.06	**M**	If data differ across different sources, the System shall display separately the data value, the source and the date of the data update (acquisition).
FR 04.07	**M**	The SRV shall prevent simultaneous processing of the same request (lock/claim).
FR 04.08	**D**	The SRV shall allow logical rollback of a decision, for authorised roles.
FR 04.09	**M**	The System shall allow importing data on the exercise of the electoral right upon completion of the election. The function shall allow verification of the update process and identification of exceptions/errors.

UC05: Extraction of information from the SRV

UC05 is the SRV capability to allow searching by role-permitted criteria, accessing the voter's profile with current and historical data, performing actions according to the role, and generating and exporting configurable reports, while preserving metadata and providing complete event logging of operations.

Table 9.5. Functional requirements for use case UC05.

Identifier	Mandatory status	Description of requirement
FR 05.01	**M**	The SRV shall allow searching by role-permitted criteria (IDNP/document, surname/forename where permitted, area, status, etc.).
FR 05.02	**M**	The SRV shall display results with pagination/filtering/sorting and configuration of visible fields per role.
FR 05.03	**M**	The SRV shall allow access to the voter's profile with current data plus pertinent history.
FR 05.04	**M**	The SRV shall allow actions from the list according to the role (transfer, status as permitted, conflicts).
FR 05.05	**M**	The SRV shall allow the creation of saved search/report templates for authorised users.
FR 05.06	**M**	All actions of report generation and data export shall be recorded in the event log.

UC06: User, role, user group and rights administration

UV06 details the functionalities for defining user access rights to user interface components, data or documents, and specifies the behaviour of UI components in interactions with authorised users.

Table 9.6. Functional requirements for use case UC06.

Identifier	Mandatory status	Description of requirement
FR 06.01	**M**	The System shall provide the functionalities necessary for managing groups/roles and their associated rights, which are to be subsequently assigned to authorised users.
FR 06.02	**M**	Any account shall be considered active from the moment of the first successful authentication except for the accounts described in FR 06.19.
FR 06.03	**M**	The user groups shall be defined at the implementation stage, but shall contain at least the following: - Administrators - Audit/Security/Supervision - CEC - View - CEC – DEC – View - Registrars - Voters – authorised external users (through MPass)
FR 06.04	**M**	The System shall incorporate a SuperAdministrator account, which will be used only for critical activities: - Modification of groups - Modification of roles - Modification of event logging parameters - Modification of cryptographic keys and access to the event archive - Creation of local accounts - Other activities defined during implementation.
FR 06.05	**M**	Each user group shall have a defined profile comprising certain roles and levels of access, including at menu level, and specific functions (e.g., data export).
FR 06.06	**M**	Distinct security requirements shall be defined for each user group. The security requirements shall be configurable and shall include at least: - Session timeout - Authentication methods - Account validity period (inactivity period until lockout) - Password requirements (complexity, validity period, expiry, history, lockout after attempts) - Device requirements (where applicable) - Other identified requirements
FR 06.07	**M**	Access rights to the system's functionalities, user interface and database records shall be defined by the user's associated group/role or explicitly for each individual user.
FR 06.08	**M**	Through the UI, the System shall allow the creation of templated profiles/roles, which may later be reused to create specific concrete roles.
FR 06.09	**D**	The System shall retain the state (history) for each role, allowing rights and actual functions to be compared at any time.
FR 06.10	**D**	The System shall allow viewing the members of any group for any time interval.
FR 06.11	**M**	Only users with administrator rights shall be able to make changes to rights, roles, groups and profiles.
FR 06.12	**M**	Any change to roles, groups, profiles and security parameters shall incorporate the principle of authorisation, therefore the action must be authorised by an account from the - Audit/Security/Supervision group.
FR 06.13	**M**	The System shall import user accounts from SAISE Admin, enabling roles to be assigned to each account either by group membership or individually.
FR 06.14	**M**	The SRV ensures integration with SAISE Admin to manage accounts, assign roles and place them into groups. Accordingly, account administration

Identifier	Mandatory status	Description of requirement
		(creation/activation/deactivation/locking/unlocking), authentication methods, etc., shall be managed via SAISE Admin.
FR 06.15	**M**	The System shall not allow the deletion of accounts, except for those that have not yet been activated.
FR 06.16	**M**	For this category of functional requirements (actions), extended detailed event logging shall be ensured. Security logs for the given UC shall be stored in encrypted form and may be accessed only through the built-in system account.
FR 06.17	**M**	Any operations on user accounts (excluding external accounts) will be accompanied by the sending of a notification email about the actions performed.
FR 06.18	**M**	MPass will be used for authentication of local and external users and for granting access rights.
FR 06.19	**M**	The System shall recognise accounts from SAISE Admin, assigning a distinct internal role to each recognised account from SAISE Admin. Accounts from SAISE Admin shall be activated manually by an administrator, with a role and group assigned to them.
FR 06.20	**M**	The System shall provide the administrator with a mechanism to assign the roles and access rights defined in the SRV to users registered in SAISE Admin and MPass.
FR 06.21	**M**	Upon authentication via MPass, the user will be offered the option to select the role of “voter” or “CEC employee”, and shall be directed to the menu and access level corresponding to that role.
FR 06.22	**M**	The SRV shall apply territorial/functional restrictions for certain roles (e.g. a registrar sees only data relating to their area of responsibility; operators see only the information for the polling station where they work).
FR 06.23	**M**	The SRV shall provide the possibility to integrate with an external authentication and authorisation mechanism (SSO/IdP).

UC07: Administration of classifiers, controlled lists and metadata

Functional requirements describing the system’s capability for working with classifiers and controlled lists. These functionalities apply only to administrative accounts.

Table 9.7. Functional requirements for use case UC07.

Identifier	Mandatory status	Description of requirement
FR 07.01	**M**	The SRV shall manage the controlled lists/classifiers used by the system.
FR 07.02	**M**	The System shall provide the authorised user with functionality to manage controlled lists and metadata.
FR 07.03	**M**	The SRV shall support importing/updating official classifiers (CUATM, addresses, etc.).
FR 07.04	**M**	The SRV shall manage mapping tables for normalisation.
FR 07.05	**M**	The SRV shall prevent the deletion of metadata that is used and shall retain history/versioning for all classifiers/controlled lists.
FR 07.06	**M**	Changes to controlled list values must not affect historical data referring to those values.
FR 07.07	**M**	When adding a new value, the start date of the validity period must be specified. The start date of the validity period may be a future date. At the same time, backdated changes shall be restricted.
FR 07.08	**M**	If there are controlled lists with elements that may change certain parameters over time, unchanging values shall also be used in addition to the record identifier provided by the database.

Identifier	Mandatory status	Description of requirement
		An example of such a case is the classifier of localities, in which localities may, over time, change their territorial subordination (district, affiliation to a locality). To preserve correct values in such cases, it is also necessary to use the unique identifier provided by CUATM. Thus, a locality may exist in the classifier in several records with different record identifier values, yet retain the same CUATM identifier. For such cases, the start date and end date of the validity period must be specified.
FR 07.09	**M**	Detailed logs shall be generated for all actions involving classifiers and controlled lists.

UC08: Data exchange with external applications

This use case describes the mechanisms the SRV uses to interact with other information systems owned and used by the CEC. The list of internal systems that will interact and the manner of interaction shall be defined at the development phase based on the data provided in the Annex to this document. In addition to the mechanisms for connecting to MConnect, the System shall also provide for and allow the connection of new interfaces when necessary.

Table 9.8. Functional requirements of use case UC08

Identifier	Mandatory status	Description of requirement
FR 08.01	**M**	The System shall ensure interoperability mechanisms with external systems via MConnect and the CEC's WSO2 DSS interoperability platform.
FR 08.02	**M**	The System shall have mechanisms for acquiring data from CEC systems and external ones that are not interoperable through MConnect and WSO2 DSS, in at least the following ways: - By direct integration via the API (web services) provided by the external application - By using ETL mechanisms to extract data directly from the databases.
FR 08.03	**M**	The SRV shall ensure interoperability with third-party external systems through MConnect. The datasets and other aspects shall be defined jointly with the Beneficiary at the implementation stage,in accordance with UC03: Automated data updating and management from external sources.
FR 08.04	**M**	The SRV shall adhere to the security and interoperability requirements of the third-party system it integrates with.
FR 08.05	**M**	The System shall ensure the management of access rights to external systems and of those from external systems, in accordance with the security requirements applied to SRV and SAISE data and the requirements of the legislation in force, including the GDPR.
FR 08.06	**M**	All data exchanges relating to personal data, both to and from the SRV, shall be recorded in the Register of Access to Personal Data.
FR 08.07	**M**	The SRV shall expose services/APIs for authorised systems. Where possible, the use of web service APIs shall be preferred.
FR 08.08	**M**	The CEC shall administer the partner systems/institutions and their rights within the SRV.
FR 08.09	**M**	The System shall allow authentication for API services with the OAuth2 authentication standard (or another agreed with the CEC), to consider including SAISE Admin" as the authentication and authorisation service for WSO2 DSS.
FR 08.10	**M**	The SRV shall support versioning of APIs and shall ensure backward compatibility for planned and controlled changes. The APIs shall be configurable and shall not

Identifier	Mandatory status	Description of requirement
		require further involvement of the developer. The developer shall provide detailed manuals.
FR 08.11	**D**	Where supported, authentication shall be provided by applying Single Sign-On mechanisms.
FR 08.12	**M**	The System shall ensure logging of each connection, while recording at least the following information: - The timestamp when the request was initiated; - Information about the user who initiated the connection; - Name of the service/API, MConnect flow or ETL that was invoked; - Status of the request (success, error, standby); - Number of rows returned; - Duration; - Error content, if it occurred.
FR 08.13	**M**	The System shall provide a set of predefined reports enabling users with administrator roles to monitor data exchange with external systems and the reuse of reusable government platform services.
FR 08.14	**M**	When interacting with external systems, the SRV shall primarily use the data definitions set out in the MConnect semantic catalogue. If necessary, modification of the MConnect semantic catalogue shall be negotiated.
FR 08.15	**M**	The SRV shall ensure the controlled import of information on participation in voting, upon completion of elections. To this end, the SRV will connect to the DB of IS "E-Day" via WSO2 DSS.

UC09: Event logging and management

UC09 defines specific details for the system's capability to log events generated in the system. These requirements are/may be complemented by other specific requirements within other UCs that address logging directly or indirectly.

Table 9.9. Functional requirements of use case UC09.

Identifier	Mandatory status	Description of requirement
FR 09.01	**M**	The SRV shall provide an interface for viewing/searching/exporting logs for authorised roles.
FR 09.02	**M**	The SRV shall generate alerts for security and operational events. Alerts and notifications shall be configurable by administrative accounts with the respective role, based on the logs configured for collection.
FR 09.03	**M**	Any event generated within the SRV may be recorded and saved in local event logs and in MLog. The SRV shall allow selecting which events are to be recorded in the event log, and which are not. The system shall ensure granular integration of events into MLog.
FR 09.04	**M**	The SRV shall generate configurable logs, with adjustable levels of detail according to the operational needs. The System shall support predefined log configuration sets, including: - Minimal – strictly logging critical events (fatal errors, system shutdowns). - Standard/Operational – logging normal operational events (authentications, data access, import/export operations). - Debugging/Development – detailed logging of internal processes (technical messages, parameters, function executions), used during testing and debugging.

Identifier	Mandatory status	Description of requirement
		- Security/Audit – logging sensitive actions (data modifications, access to confidential information, configuration changes), retaining metadata about user, time and device. - Custom – flexible configuration by the administrator, with the ability to define the fields and events that must be recorded in the event log. The System shall allow real-time changes to the logging level without interrupting operation, and shall retain the history of the configurations applied. Each of the predefined sets may be adjusted, with the option to save it as a new customised set.
FR 09.05	**M**	Logged events shall store at least the following categories of data (depending on the nature of the event logged): - the identifier of the logged event; - the identifier of the user who generated the event; - the type of action performed (creation, modification, deletion, access); - the timestamp of the event's occurrence / of its logging; - the location of the impacted resource (e.g. the record ID) - the application component that generated the business event; - the outcome of the action (e.g. success, failure) and the reason in case of a failure, etc.
FR 09.06	**M**	Archiving and retention: - Logged events must be kept for a configurable period (12 months by default). - The System must allow automatic archiving of logged data without affecting performance. The frequency, execution time, and other parameters for performing archiving - Events may be archived to the default location or to the specified location.
FR 09.07	**D**	The System shall incorporate tools to encrypt both archived and current logs, applying secure encryption algorithms. Management of encryption parameters may be assigned to one or several specific accounts.
FR 09.08	**M**	Event logging must comply with applicable legislation on the protection of personal data (e.g. GDPR) and the audit requirements specified in national regulations.
FR 09.09	**M**	The Contractor shall ensure integration of the system with the internal SIEM system, according to the criteria defined during implementation.
FR 09.10	**M**	The Contractor shall ensure the system's integration with the governmental MLog service.
FR 09.11	**M**	From the administrator menu, the System shall permit configuring the categories of events to be recorded additionally via MLog.
FR 09.12	**M**	Logging shall use a structured JSON format and shall be collected in accordance with the K8s pipeline: FluentBit - Kafka - OpenSearch/Kibana (MLog). Logs shall comply with the standard MLog fields.

UC10: Extraction of statistics and reports

This UC sets out the Requirements for the system's capability to manage the retention (generation) of data required for statistical and reporting activities, across all segments (data, views, imports and exports, synchronisations, etc.). Typical reports and reports defined during system operation shall be based on existing data, or data generated following analysis of the information contained in the Register.

Table 9.10. Functional requirements of the UC10 use case

Identifier	Mandatory status	Description of requirement
FR 10.01	**M**	The SRV shall provide reports/statistics according to the defined roles and criteria.
FR 10.02	**M**	The SRV shall include predefined reports (country/district/municipality/locality/polling station) and real-time election-day turnout to public websites.
FR 10.03	**M**	Reports shall be generated on the basis of data from the SRV and relevant information obtained from SAISE. The SRV shall import and retain the data used to define and generate the reports.
FR 10.04	**M**	The System shall allow the creation of report templates, based on available data and data eligible for import from the SAISE TechDB, or aggregated information derived from these data.
FR 10.05	**D**	The SRV shall generate data quality reports (e.g. missing fields, conflicts, unassigned addresses, controlled list errors), useful for administration.
FR 10.06	**M**	The System shall enable CEC users to generate reports based on the defined criteria. The SRV shall allow the generation and export of reports in accordance with data export rights (a configuration criterion for the categories of data that may be downloaded by the user). Reports may be viewed on screen, or exported in formats (CSV, XLSX, XML/JSON, PDF).
FR 10.07	**M**	The system shall retain a copy for each report generated or exported, including metadata about who, when and from which device it was created/generated/exported.
FR 10.08	**M**	The option to extract and export data may be configured granularly by the administrator based on user groups or named user accounts (e.g. only for a polling station). These configurations shall be done through the UI, with no need to modify or write code, or commands.
FR 10.09	**M**	When granting access rights, it shall be possible to customise (for each named account or user group) the fields available for viewing and/or export.
FR 10.10	**M**	The System shall include a module for report management and data export. All functions intended for report management shall be available through the UI, without the need to write or modify code, or to operate with DB commands.
FR 10.11	**M**	The report management module shall incorporate functionality for building, formatting and editing templates.
FR 10.12	**M**	Upon modification of any report template, the previous version shall also be retained, with all necessary metadata (date, account used, etc.).
FR 10.13	**M**	The System shall allow creating any report templates based on the data available in the DB, applying additional criteria or parameters (e.g. period, age, sex, etc.).
FR 10.14	**M**	Access to any report template may be granted at a granular level, based on user groups or named accounts.

UC11: Assignment and management of polling stations

UC11 is the SRV capability to assign a polling station based on the address and established rules, allow mass or individual assignment, transfer voters between stations, manage assignment conflicts, as well as import and keep the history of polling station states.

Table 9.11. Functional requirements for use case UC11.

Identifier	Mandatory status	Description of requirement
FR 11.01	**M**	The SRV shall assign the polling station based on the address, the controlled list of stations and the established rules (including the "single station" case).

Identifier	Mandatory status	Description of requirement
FR 11.02	**M**	The SRV shall allow mass assignment of the station (by locality/streets/address) and individual assignment for a voter.
FR 11.03	**M**	The SRV shall allow the transfer of voters between stations, in line with institutional rights and constraints.
FR 11.04	**M**	The SRV shall detect and manage assignment conflicts (address without a station, non-existent station, etc.), providing the reason and a list of errors/conflicts.
FR 11.05	**M**	The SRV shall allow previewing the impact of reassignment (number of voters affected) before applying it.
FR 11.06	**M**	The System shall allow importing polling stations in an agreed/predefined format. When importing data on polling stations, before applying it, the System shall require confirmation from the administrator. Each import of polling station data shall constitute a “State”, which shall have a unique identifier.
FR 11.07	**M**	The System shall retain the application history for all "States", with the necessary technical information.
FR 11.08	**M**	The System shall allow exporting and generating detailed reports on polling stations, including information on the addresses to which they are assigned for any of the elections registered in the system. Note: the structure and description of the report fields will be provided at the implementation stage.
FR 11.09	**M**	The SRV shall ensure functionality to generate the boundaries in Word format, as a table with a predefined template, with the option for municipal registrars to download it, to be used (the SRV boundaries) in the order concerning the establishment of Polling Station boundaries.
FR 11.10	**M**	The System shall allow exporting and printing information about the boundaries (included addresses) of a polling station or several polling stations, selected manually. When generating reports, data about the datasets used (election, address State ID, etc.) will also be presented.
FR 11.11	**M**	The SRV shall allow the generation of documents (tables relating to polling stations) with a defined, adjustable structure, ensuring A4 compatibility.
FR 11.12	**M**	The SRV shall allow exporting reports in standard formats (PDF/CSV/XLSX) and retaining versions by period/election.
FR 11.13	**M**	The SRV shall allow graphical (map) viewing of station boundaries and voter distribution.

UC12: Generation and export of electoral rolls

UC12 is the SRV capability to generate and export the electoral rolls to SAISE (e-Day), in line with schedules and approved rules, with prior validation, error and version management, detailed event logging, and retention of export history.

Table 9.12. Functional requirements for use case UC12

Identifier	Mandatory status	Description of requirement
FR 12.01	**M**	1. The SRV shall generate and export the electoral rolls to SAISE (e-Day) automatically, in accordance with the approved schedules and rules. 2. The export procedure is required to be very fast and to allow stopping and resuming the process. 3. The export may be performed repeatedly. 4. The export can be performed based on criteria, and in full, differential, or synchronisation/update mode.

Identifier	Mandatory status	Description of requirement
FR 12.02	**M**	The SRV shall display the export stages and retain the complete history (jobs, versions, status, errors).
FR 12.03	**M**	The SRV shall perform pre-export data validation and, upon critical errors, stop the export and issue a validation report.
FR 12.04	**M**	The SRV shall allow stopping, re-running failed exports, and retaining the exported differences/versions.
FR 12.05	**M**	Detailed reports including the necessary technical details shall be generated automatically for export operations.
FR 12.06	**D**	The System shall allow detailed event logging (at record level) of operations for generating, exporting and printing electoral rolls.
FR 12.07	**M**	The System shall allow generating, exporting or printing the electoral roll(s) for: - one polling station - several polling stations - one locality or several localities - one election or more - based on criteria defined at the implementation stage (e.g., by number of voters, etc.) - The System shall allow performing operations on the rolls for different types of elections distinctly, without affecting functionality or the related workflows.
FR 12.08	**M**	When exporting or printing the electoral rolls, the System shall generate mandatory metadata to identify relevant details (user, time, format, the version and ID of the addresses used, and other identifiers needed for audit and traceability).
FR 12.09	**M**	The System shall retain the history and version of data (rolls) exported or printed according to adjustable parameters: - for a period - for an election - number of states/versions - by whom it was generated - ID of the “state” of address information used.
FR 12.10	**M**	The System shall allow verifying the electoral roll by IDNP.
FR 12.11	**D**	The System shall allow verifying the electoral rolls based on a set of IDNP imported in XML file format or on external queries via API.

UC13: Address management and normalisation

UC13 represents the SRV capability to unify and normalise addresses, prevent semantic duplications, allow the creating, modifying and mapping of addresses with the SRP, validate and manage conflicts, perform geolocation and audit changes, and administer address states and history through dedicated roles and mandatory justification mechanisms.

Table 9.13. Functional requirements for use case UC13

Identifier	Mandatory status	Description of requirement
FR 13.01	**M**	The SRV shall manage the unification and normalisation of addresses and shall prevent semantic duplication of addresses.
FR 13.02	**M**	The SRV shall allow creating/modifying addresses/streets and SRV-SRP mapping, including selecting the polling station and necessary codes.
FR 13.03	**M**	The SRV shall validate the uniqueness and consistency of addresses and shall manage address conflicts.
FR 13.04	**M**	The SRV shall allow geolocating addresses on a map and auditing address changes.

Identifier	Mandatory status	Description of requirement
		Geolocation will rely on geolocation platforms and services, following the integration protocols and standards agreed during the implementation process.
FR 13.05	**M**	The SRV shall allow viewing address details from the perspective of: - change history (with the date and the source/reason specified) - the source of the information and the information date - comments and support notes (e.g. version in Cyrillic characters, others) - the presence of any conflicts or duplications.
FR 13.06	**M**	For each object in the information on addresses, the SRV shall create a unique identification code, which shall be displayed as necessary, according to the agreed scenarios.
FR 13.07	**M**	The System shall allow setting a "state" for addresses and using it to generate reports, export lists, etc. The System shall retain sufficient details about the "state" of the information about an address (or address record) so that each piece of data can be associated with the source and the date from which it applies (e.g. street name obtained from the SRP, sector corrected by the address administrator as of the given date, etc.).
FR 13.08	**M**	The System shall include a predefined specific role "Address Administration", which may be assigned to specific accounts. The account shall have predefined functions and the necessary permissions for conflict management, data adjustment, etc.
FR 13.09	**M**	The System shall require the completion of text fields and the attachment of documents for any manual intervention on addresses. The System shall require a reason or justification field to be completed before allowing changes.
FR 13.10	**M**	The System shall allow fixing, at a point in time, the "state" of data on addresses, so that these states can be used/reused. Each "state" shall have a unique ID, which will also be used in other operations (e.g. exporting or printing electoral rolls, defining polling stations, etc.).
FR 13.11	**M**	The System shall allow updating/reconciling all addresses, or based on at least the following criteria: 1. For certain sets (lists) of addresses 2. For certain localities or territorial units (districts, municipalities, etc.) 3. Left bank of the Nistru River 4. A certain age 5. Certain types of identity documents 6. Issue date range for the identity document 7. Other criteria to be defined at the development/implementation stage
FR 13.12	**M**	For each election, the System shall allow generating detailed reports about addresses pertaining to one or several polling stations.

UC14: Correction and management of voter data

UC14 is the SRV capability to allow the correction of voter data based on supporting documents, with mandatory justification, retention of history and states, viewing of the complete profile, and controlled rollback of changes.

Table 9.14. Functional requirements for use case UC14

Identifier	Mandatory status	Description of requirement
FR 14.01	**M**	The SRV shall allow correcting certain data and identifying erroneous data.
FR 14.02	**M**	The SRV shall allow modifying the voter status based on a supporting document. Any modification shall require a justification of the action:

Identifier	Mandatory status	Description of requirement
		- Reason / justification. The reasons shall be managed based on a controlled list, with the possibility to add/modify/delete certain reasons. - Case description - Attachment and record of document(s) – similar to FR 04.01. - Comments / remarks
FR 14.03	**M**	The SRV shall display the voter's complete profile (data, history, documents, addresses, polling stations, attendance, etc.). The System shall allow viewing voter data at a point in time, aligned with other datasets valid on the selected date (polling stations, addresses, etc.). The System shall allow viewing the historical data relating to a voter (their previous addresses, statuses, etc.).
FR 14.04	**M**	The SRV shall allow a controlled reversal of a change (logical rollback). The operation shall be accepted only after the reason has been provided and full traceability of actions is ensured.
FR 14.05	**M**	The System shall retain detailed logs of every activity/action on voter data.

UC15: Management of alerts and notifications

UC15 is the SRV capability to configure notification messages and channels, manage alerts and delivery rules without code changes, view and filter notifications with their resolution history, and link notifications to relevant entities.

Table 9.15. Functional requirements of use case UC15.

Identifier	Mandatory status	Description of requirement
FR 15.01	**M**	The System shall allow configuring the displayed messages and the notification method for each case. The SRV shall allow configuring notification channels (system interface, email, API).
FR 15.02	**M**	The SRV shall allow viewing, filtering and managing notifications, including details and resolution history.
FR 15.03	**M**	The system shall provide configurable alerts and notifications for all scenarios requiring authorisation, acceptance, coordination, or similar actions.
FR 15.04	**M**	The System shall allow selecting specific events for alert generation.
FR 15.05	**M**	The System shall allow configuring the delivery method for each alert and the list of recipients. Alerts shall be sent to a group of users or to a configurable list of accounts. The following delivery methods for alerts shall be available at a minimum: - E-mail (from the targeted user's or group's profile) - In the command bar as a system message or notification - As a pop-up in the application interface
FR 15.06	**M**	The SRV shall allow defining notification trigger (delivery) rules without code changes.
FR 15.07	**M**	The System shall have the capabilities to provide notifications to system users and requesters regarding the occurrence of specific events. The list of specific events shall be finalised at the implementation stage. The System shall allow editing the list of active notifications via the UI, without the need to modify the code.
FR 15.08	**M**	The SRV shall allow configuring notification types and display rules per role.
FR 15.09	**M**	The SRV shall allow marking notifications as read/unread and archiving them.

Identifier	Mandatory status	Description of requirement
FR 15.10	**M**	The System shall have the capability to track whether the recipient has received the notification (for notifications sent via the SRV) and to inform the initiator (if the notification was initiated by a human user).
FR 15.11	**M**	The SRV shall generate automatic notifications for critical events (conflicts, errors, sensitive changes, failed jobs).
FR 15.12	**M**	The SRV shall allow prioritisation of notifications (critical, important, informational).
FR 15.13	**M**	The SRV shall correlate notifications with relevant entities (voter, conflict, job, export).
FR 15.14	**M**	The SRV shall log the handling of notifications (who viewed, who resolved).
FR 15.15	**M**	The system shall be integrated with the MNotify government service and shall ensure event management through this service.

UC16: Management of Declarations of Residence and the request to vote at the place of stay, as well as issuance of the voting rights certificate

UC16 represents the RSV capability to create, validate, and manage documents intended for voters—namely: (a) declaration of residence, (b) request for voting at the place of stay, and (c) voting rights certificate—for an electoral process. This includes verification of voter eligibility, enforcement of document uniqueness, mandatory cross-checking against RSV data, generation, electronic signing, and PDF export, attachment to the voter's profile, versioning and metadata retention, generation of reports and notifications, as well as establishment of the registration deadline. UC16 shall be applicable exclusively to users authenticated via MSign.

Table 9.16. Functional requirements for use case UC16

Identifier	Mandatory status	Description of requirement
FR 16.01	**M**	The SRV shall allow the management of user documents for an electoral process, including verification of voter data and eligibility rules: (a) declaration of residence, (b) request for voting at the place of stay, (c) voting rights certificate. The documents and corresponding functionalities shall be available only to voters authenticated via MPass.
FR 16.02	**M**	All documents shall have several states in the system, which will be managed based on specific parameters or actions performed on them. The document states are: - Draft - Signed (by the voter) - Withdrawn (by the voter) - Cancelled (by the voter or the CEC) - Expired (referring to a previous/completed electoral process)
FR 16.03	**M**	The RSV shall provide functionality for creating and signing requests addressed to voters for the expression of the right to participate in elections (voting) at the place of stay (FR 16.03), applicable only for the upcoming electoral process. Accordingly, these documents shall be valid only for the next election for which the request was made, provided they were created within the deadline established by the CEC for each document type.
FR 16.04	**M**	The system shall allow, for each electoral process and for each document type, the configuration of the following parameters: - Start date from which requests may be submitted - Deadline until which requests may be submitted

Identifier	Mandatory status	Description of requirement
		- Deadline until which documents may be signed by the voter - Validity period - Minimum document age (time interval between requests submitted by the same person) Each document shall be considered valid from the moment it is signed by the voter.
FR 16.05	**M**	The system shall allow only one residence declaration and one request for exercising the right to vote at the place of stay per person. Should the person wish, these declarations may be cancelled within the established timeframe (configurable value). Documents subject to any constraints (e.g., maximum number of requests accepted per polling station, etc.) may be signed and considered valid only if such limits are respected. In case the limits are exceeded, the system shall not allow the creation and/or signing of the document (depending on its status), and shall display a corresponding message to the user.
FR 16.06	**M**	For each document type, the system shall allow the definition of quantitative limits, both at a general level (per document type) and per polling station.
FR 16.07	**M**	The quantitative limit per polling station shall be calculated based on documents in the Active Signed state (excluding Withdrawn/Cancelled/Expired). Upon withdrawal or cancellation of a document, the available capacity (based on the defined limit) shall be automatically recalculated and restored.
FR 16.08	**M**	The system shall allow only one document of each type per person for each electoral process. When creating a document, the system shall verify the existence of any other document (uniqueness) of any of the types mentioned. If such a document exists for the same electoral process, the system shall inform the user of its existence. In order to proceed with the creation of a new document, the system shall require the user to confirm the cancellation of all previous documents, regardless of their current status, before initiating the creation of a new document.
FR 16.09	**M**	The RSV shall enable the generation, signing, and export of documents in PDF format, as well as their attachment to the voter's profile within the RSV. In EVO, only information regarding the existence of the document and its status shall be displayed. The system shall maintain versioning of generated file data and metadata.
FR 16.10	**M**	Minimum fields for the Declaration of Residence: - name of the second-level administrative-territorial unit, as appropriate; - type of administrative-territorial unit (municipality, town, commune, village); - name of the locality (municipality, town, commune, village); - sector, street, house number, block, flat number, as appropriate.
FR 16.11	**M**	The RSV shall enable and obligatorily perform the cross-checking of information from the voter's declaration of residence and request to vote at the place of stay, as completed by the voter, against the most recent data available in the RSV. The registrar responsible for processing the declaration shall be alerted to any discrepancies identified between these documents and the RSV data and shall be informed (notified) of the outcome of their action if the information from the declaration is retained.
FR 16.12	**M**	The System shall allow repeated assignment of the voter after registering the declaration of residence.

Identifier	Mandatory status	Description of requirement
FR 16.13	**M**	The system shall allow the generation of parameterized reports on residence declarations/documents (e.g., period, administrative-territorial unit, status, locality, etc.).
FR 16.14	**M**	The system shall generate notifications in the EVO mobile application (for citizens who have it), in the EVO personal web cabinet, and in the RSV personal cabinet regarding any actions related to documents, as well as changes in polling station allocation.
FR 16.15	**M**	In the voter's cabinet, and identically in the citizen's EVO cabinet, all data related to documents, their status, document history, and user operations on them shall be displayed based on data from the RSV.
FR 16.16	**M**	The system shall allow the creation of new templates and/or the reuse of existing templates for each document type and for each electoral process.
FR 16.17	**M**	The system shall retain all user documents created within the system, together with the necessary metadata to define document details and their status over time.
FR 16.18	**M**	The system shall allow the generation of QR codes intended for document identification and verification within the system.
FR 16.19	**M**	The document workflow is described as follows: - The voter requests the document in the system based on the template loaded for the current electoral process. - The system checks for the existence of other documents and verifies compliance with the established limits and parameters. - The voter completes the mandatory fields. All fields shall include validation and verification functions against existing system data. - The system checks for conflicts or other mandatory criteria and notifies the user where applicable. - The voter signs the document using MSign, confirming responsibility for the document and its signing, as well as any related implications arising from the system logic. - After the document is signed, the issuance is recorded in the system, including in the voter lists for the polling station where it was signed. - Each document shall have a unique ID, which may be represented in the form of a QR code. - The existence of the document shall be reflected in the RSV personal cabinet and in EVO. Note: Mandatory fields will be defined during the implementation phase.
FR 16.20	**M**	Registrars and other roles to which this function is assigned shall be able to verify information about a citizen's documents based on the personal identification number (IDNP). In this regard, the system shall display the status of the documents and the dates of operations performed on these documents.
FR 16.21	**M**	The system shall cancel all documents at the end of the electoral process. Accordingly, RSV shall automatically reassign the voter to their domicile or residence address upon completion of the electoral process.

UC17: Ensuring compatibility with different types of elections

The UC17 functionality aims to ensure the SRV's compatibility with different types of election and the governance of their parameterisation, so that the system can operate in a controlled and differentiated manner for local, presidential, parliamentary, regional elections, republican or local referendums. Scenarios in which several types of election take place simultaneously must be considered (e.g., parliamentary elections and a

referendum). The SRV shall allow “per election” configuration of periods, rules, statuses and the set of available reports, as well as defining rules specific to the election type (eligibility, special polling stations, lists, validity period of domicile/residence registration), with the ability to enable/disable functionalities depending on the selected option.

Table 9.17. Functional requirements for use case UC17

Identifier	Mandatory status	Description of requirement
FR 17.01	**M**	The SRV shall support the conduct of different types of election (local, presidential, parliamentary, referendum, or other types) in accordance with national legislation and the CEC regulatory framework.
FR 17.02	**M**	The SRV shall allow managing configurations per election and by type of election (periods, rules, statuses, reports, etc.).
FR 17.03	**M**	The SRV shall allow defining rules specific to each election type (eligibility, special polling stations, lists, publication terms, etc.).
FR 17.04	**M**	The SRV shall ensure activation/deactivation of functionalities according to the selected election type.
FR 17.05	**M**	The SRV shall allow the simultaneous management of multiple elections (history + active election).
FR 17.06	**M**	The SRV shall allow running several elections of different types held concurrently (e.g., parliamentary elections and a referendum). The elections shall be managed in parallel without functional or performance impact on any of them.
FR 17.07	**M**	The SRV shall retain historical election configurations for audit, reporting and analysis.
FR 17.08	**M**	The SRV shall log configuration changes per election.
FR 17.09	**D**	The SRV shall allow simulating electoral scenarios (impact on lists and polling stations).

UC18: Conflict management

The UC18 functionality seeks to implement in the SRV an end-to-end framework for data conflict management, aiming to detect, record, analyse and remediate in a controlled way inconsistencies arising when processing and synchronising the information (address/polling station/street/status types, missing CUATM codes, discrepancies including those from the SRP and TechDB). The System shall present the differences in a comparative manner (SRV vs external source) for decision support, manage the conflict lifecycle (new/in progress/resolved/rejected) with assigned responsibility, and allow governed resolutions through actions specific to the conflict type (assign an existing address, create a new address, metadata corrections, status decisions). UC21 requires collaboration between authorised roles through sharing: providing a reason and a note, attaching documents and maintaining the full history for traceability/audit, as well as control via a "claim/lock" mechanism that eliminates simultaneous processing of the same conflict. Optionally, prioritisation rules for triage may be defined according to impact and urgency. This functionality complements (and is complemented by) other specific requirements stipulated in these Terms of Reference. Although certain functional aspects are similar across different UCs, the System shall contain a separate module and menu dedicated to UC18.

Table 9.18. Functional requirements for use case UC18

Identifier	Mandatory status	Description of requirement
FR 18.01	**M**	The SRV shall identify and record conflicts arising in data processing (address, polling station, street, status, missing CUATM/codes, inconsistencies), including from synchronisations with the SRP, the TechDB and other external sources.
FR 18.02	**M**	The SRV shall display conflict details side by side (SRV data vs external source data/TechDB) for analysis of differences.
FR 18.03	**M**	The SRV shall allow managing the conflict lifecycle: new/in progress/resolved/rejected, assigning a responsible person (where appropriate).

Identifier	Mandatory status	Description of requirement
FR 18.04	**M**	The SRV shall allow resolving conflicts through controlled actions, depending on type: assign existing address, create new address, correct metadata, decide status, etc.
FR 18.05	**M**	The SRV shall allow sharing conflicts between registrars/authorised roles, selecting a reason (controlled list) and adding a note.
FR 18.06	**M**	The SRV shall allow attaching documents/notes to the conflict and retaining the full history of actions on it.
FR 18.07	**M**	The SRV shall prevent simultaneous processing of the same conflict by multiple users (using a "claim/lock" mechanism).
FR 18.08	**M**	The SRV shall allow defining prioritisation rules for conflicts (e.g., impact on the right to vote, volume, origin, deadline). The SRV shall allow generating reports based on conflict types or other characteristics (e.g. frequency, recurrence, etc.).
FR 18.09	**M**	The SRV shall allow setting/assigning, for any type of conflict, those responsible for review and coordination/acceptance (role-based or nominally per user account).
FR 18.10	**M**	The list of conflicts and other inconsistencies shall be viewable through the application interface and may be exported in the selected format (CSV, XLSX, XML/JSON, PDF).

UC19: Administration of Interop (Interoperability) functionalities

The UC19 functionality establishes in the SRV a dedicated interoperability module ("Interop") for governing integrations with external systems, covering administration of interconnected systems, partner institutions, and the transactions exchanged between parties. The SRV shall allow registering and maintaining external systems (identifier, type, purpose, environment, active/inactive state), managing institutions and their association with interfaces/systems, and configuring permissions granularly by external system and transaction type (read/write) in accordance with approved policies. Operationally, the SRV ensures viewing of transactions with the minimum necessary details (request/response, status, errors, timestamps, calling system), with filtering and search capabilities for diagnostics, plus definition of the processing mode (manual vs automatic) per integration, where relevant; optionally, a controlled export of Interop logs is envisaged for investigations and audit to maintain end-to-end traceability and accountability.

Table 9.19. Functional requirements for use case UC19

Identifier	Mandatory status	Description of requirement
FR 19.01	**M**	The SRV shall include the dedicated Interop module for the administration of Systems, Institutions and Transactions.
FR 19.02	**M**	The SRV shall allow registering and managing interconnected systems (identifier, type, purpose, environment, active/inactive state).
FR 19.03	**M**	The SRV shall allow managing partner institutions and their association with systems/interfaces.
FR 19.04	**M**	The SRV shall allow configuring permissions per external system and per transaction type (read/write), in accordance with approved policies.
FR 19.05	**M**	The SRV shall allow viewing transactions (minimal request/response, status, errors, timestamps, calling system), with filtering and search.
FR 19.06	**M**	The SRV shall allow defining the processing mode of transactions (manual/automatic) per integration, where relevant.
FR 19.07	**D**	The SRV shall allow controlled export of Interop transaction logs for investigations/audit (according to permissions).

UC20: Management of attached files

The UC20 functionality introduces in the SRV a mechanism for managing attached files, intended to support actions with documentary evidence and to ensure traceability of operational decisions. The System shall allow uploading supporting documents associated with sensitive events (such as a status change), based on permissions, and ensure their viewing both from the voter's profile and from the relevant operational objects (conflicts/changes).

Table 9.20. Functional requirements for use case UC20

Identifier	Mandatory status	Description of requirement
FR 20.01	**M**	The SRV shall allow uploading supporting documents that are non-editable by default (e.g.: PDF/JPG) associated with critical actions (e.g., status change), according to permissions. For each attached document, metadata necessary for the unique identification of the file and other details (timestamp, user, device, etc.) shall be retained. The functionality described in FR 04.01.
FR 20.02	**M**	The SRV shall allow viewing attached documents from the voter profile and from the relevant operational object (conflict/modification).
FR 20.03	**M**	The SRV shall validate the type and size of uploaded files (extension whitelist, MB limit) and shall reject non-compliant files.
FR 20.04	**M**	The SRV shall allow only authorised roles to download the attached filed and shall record all accesses in the log file.
FR 20.05	**M**	The SRV shall allow versioning of attached documents (controlled replacement), retaining the history and the reason.
FR 20.06	**M**	Documents shall be stored encrypted/protected so as to prevent operations on them from outside the system.
FR 20.07	**M**	The System shall ensure granular advanced event logging for all operations related to file handling.

10. Non-functional requirements

To describe the non-functional requirements, different specific categories and types of requirements shall be used, separated by domain. For each requirement, the mandatory status is specified: M – a requirement that must be implemented (Mandatory), D – a requirement desired to be implemented, optional (from the English term Desirable), and I – an informative requirement.

Each category is defined separately, with requirements coded according to the principle "NFR"-"Cat"."XY", where "NFR" means non-functional, "Cat" is the category abbreviation per Table 10.1, and "XY" is the sequence number. The categories of non-functional requirements, the abbreviations used, and the description of each category are presented in Table 10.1:

Table 10.1. Categories of SRV non-functional requirements

Identifier	Meaning	Category definition/description
GN	General requirements	Non-functional general requirements that apply across the board to all aspects, regardless of area and category.
LC	Licensing and intellectual property requirements	Requirements regarding the necessary licences and the rights of use/ownership over the solution and deliverables.
AH	Requirements regarding the system architecture	Requirements regarding the principles, structure and organisation of the system architecture.
TH	Requirements regarding the technologies used	Requirements regarding the permitted/recommended technologies, versions, compatibility, and the avoidance of EOL technologies.
IO	Interoperability requirements	Requirements regarding interfaces, integration and data exchange with external systems (including MConnect).
PF	Performance requirements	Requirements regarding response times, load, concurrency, and the impact of processes on performance.
EA	Ergonomics and accessibility	Requirements regarding UI/UX, accessibility (WCAG), and adapting the interface to different devices/resolutions.
SC	Security	Requirements regarding the secure design and operation of the system (secure by design, controls, data protection).
MT	Maintainability	Requirements regarding maintenance, administration, and ease of system operation/update.
SL	Scalability	Requirements regarding resource expansion and capacity growth without degrading operation.

General requirements

The general requirements set out the core conditions applicable to the entire SRV system and the entire project (working environments, resilience, efficient use of resources, open technologies and general constraints). These requirements apply transversally, regardless of component or functionality. The non-functional general requirements are defined in Table 10.2:

Table 10.2. General non-functional requirements

Identifier	Mandatory status	Description of requirement
NFR-GN.01	**M**	The Contractor shall ensure the necessary infrastructure resources for: - Development environment; - Working files and documents as part of the project.
NFR-GN.02	**I**	CEC shall provide resources for configuring the following operating environments for the SRV: - Production environment; - Testing/training environment;

Identifier	Mandatory status	Description of requirement
		The aforementioned operating environments shall be provided on the CEC platform. CEC shall provide only virtual servers with or without an operating system; the other required components shall be provided by the Contractor.
NFR-GN.03	**M**	The System shall ensure a high level of resilience to failures/outages and shall not contain single points of failure (SPOF).
NFR-GN.04	**M**	The System shall ensure rational and balanced use of processing resources.
NFR-GN.05	**M**	The technologies used must be open (no vendor-proprietary technologies).
NFR-GN.06	**M**	Components must be independent of the technology platform on which they run (unless explicitly required by these Terms of Reference).
NFR-GN.07	**M**	The technologies used must be homogeneous (a minimal number of different technologies, e.g. the same operating systems for the business logic server and databases).
NFR-GN.08	**M**	The Tenderer shall indicate in its bid full and exhaustive information regarding the technology platforms supported by its application and the relevant constraints.

Requirements regarding licensing and intellectual property

The SRV shall be built exclusively on open-code, zero-licence-cost technologies, in accordance with the requirement for open, non-proprietary solutions. No commercial software licences, per-node fees, per-user fees, or subscription-based proprietary components shall be introduced as part of the proposed solution. The CEC shall not incur any recurring or one-time software licence costs as a result of this procurement, either for the initial implementation or for future scaling of the system.

Table 10.3. Licensing and intellectual property requirements

Identifier	Mandatory status	Description of requirement
NFR-LC.01	**M**	The Tenderer shall provide a complete inventory of all software components included in the proposed solution, specifying for each: the component name and version, the applicable open-source licence (e.g. MIT, Apache 2.0, LGPL, GPL), and any obligations that licence places on the CEC as the system owner and operator. No proprietary or commercially licensed components shall be included. Any component subject to a copyleft licence (e.g. GPL, AGPL) must be explicitly identified, with an explanation of how the licence obligations are managed without restricting the CEC's ability to operate, modify, or procure maintenance for the system from a third party.
NFR-LC.02	**M**	All components shall be deployable across both the Primary Data Centre and the Disaster Recovery location in Active–Passive mode without any additional cost, restriction, or re-licensing requirement. The open-source licence of each component must permit unrestricted deployment across multiple environments and infrastructure nodes.
NFR-LC.03	**M**	The Tenderer shall confirm in writing that no component included in the solution requires a commercial licence, support subscription, or proprietary extension to function as specified in these Terms of Reference. Where a component offers both a community (open-source) edition and a commercial edition, only the community edition may be used, and the Tenderer shall confirm that the community edition fully satisfies all functional and non-functional requirements defined herein.
NFR-LC.04	**M**	The Contractor shall transfer to the CEC full and unrestricted rights over all custom-developed components, including application code, configuration scripts, integration adapters, deployment manifests, database schemas, and

Identifier	Mandatory status	Description of requirement
		any modifications made to third-party open-source components. The transfer shall be consistent with the applicable open-source licence terms of any modified components. Following transfer, the CEC shall be entitled to use, modify, extend, and procure third-party maintenance for the system without any dependency on the original Contractor.
NFR-LC.05	**M**	The complete source code for all SRV components developed under this contract shall be delivered to the CEC via the version control system (Git), with full commit history, branch structure, and inline documentation sufficient for an independent developer or team to build, deploy, and maintain the system. Source code delivery shall occur at the end of each development sprint and at final handover, not solely at project completion.
NFR-LC.06	**M**	All technical documents, descriptions, training materials, presentations, testing documentation and any other documents shall become the property of the CEC, without limiting their use. All the aforementioned documents and information, except those that were subject to intellectual property rights before the start of the project, shall constitute the CEC's intellectual property under Moldovan law. All the aforementioned documents should be in Romanian.
NFR-LC.07	**M**	The Tenderer shall describe the long-term maintainability model for the proposed open-source stack, addressing: the maturity and community activity of each core component, the availability of commercial support options should the CEC require them in the future, and the approach to managing component updates, security patches, and end-of-life transitions over the system's operational lifetime.

Requirements regarding the system architecture

The SRV architecture must be aligned with the CEC needs and the technological context of its implementation, particularly regarding scalability, extensibility, flexibility and maintenance. The CEC prefers an open, modular architecture based on interoperable components. These principles must be visible at all levels of the architecture.

General requirements

General requirements regarding the system architecture are defined in Table 10.4:

Table 10.4. General requirements regarding the system architecture

Identifier	Mandatory status	Description of requirement
NFR-AH.01	**M**	Any inconsistency or incompatibility, or optimisation option, in the technology architecture (systems, technical components, platforms, services, etc.) identified during the project shall be communicated to the CEC and UNDP, with options for resolution/handling/improvement discussed and agreed. Adjustments arising from the above shall be documented in detail, including by updating the supporting documents provided by the CEC in the context of the SRV's implementation and operation.
NFR-AH.02	**M**	The SRV architecture must be based on open standards.
NFR-AH.03	**M**	The SRV architecture must be service-oriented (SOA).
NFR-AH.04	**M**	The SRV architecture shall be designed in an integrated manner, developed using best practices in the field (for example: architecture principles and reference architectures aligned with TOGAF 9.2 / 10.0).

Identifier	Mandatory status	Description of requirement
NFR-AH.05	**M**	The SRV architecture shall be client–server, organised into at least three vertical tiers: - Presentation (client interaction) - Application logic (business/application logic) - Data access (data management / DBMS) The layers must be clearly separated, ensuring each upper layer relies only on the layer beneath it.
NFR-AH.06	**M**	The SRV architecture shall be adapted for implementation and use in virtualised environments, with no restrictions.
NFR-AH.07	**M**	Communication between all system components shall be carried out securely, using their internal interfaces for this purpose.
NFR-AH.08	**M**	The architecture must be designed to ensure the application is scalable, able to adapt to increases in user numbers and/or data volume without degrading performance.
NFR-AH.09	**M**	Fault tolerance: the software solution must be able to handle errors and recover quickly in the event of system or network failures. In the event of any interruption of connections/functions, the implemented mechanisms shall allow the automatic resumption of functionalities.

Presentation layer

The requirements regarding the presentation layer are defined in Table 10.5:

Table 10.5. Requirements regarding the presentation layer

Identifier	Mandatory status	Description of requirement
NFR-AH.10	**M**	The System shall provide user interfaces enabling the user to access a single entry point for all business functions for which they are authorised. Exceptions are allowed for roles with privileged rights (e.g., system administrator).
NFR-AH.11	**M**	Client access shall be possible from any standard operating environment, or with minimal configuration by the Beneficiary (e.g. standard system software only).
NFR-AH.12	**M**	By default the client shall access the system through any standard browser, with compatibility ensured and tested for at least: Microsoft Edge, Google Chrome, Firefox, Safari.
NFR-AH.13	**M**	The presentation layer shall not implement (incorporate) business rules, except for input data validation.

Business logic

The requirements regarding the business logic are defined in Table 10.6:

Table 10.6. Requirements regarding the business logic

Identifier	Mandatory status	Description of requirement
NFR-AH.14	**M**	The business logic layer must be entirely independent of the presentation layer and the data management layer (DBMS).
NFR-AH.15	**M**	The business logic layer must have a fully modular architecture, based on reusable components and abstract interfaces. At this layer, different components must not implement the same functionality (e.g., data access).
NFR-AH.16	**M**	Business entities (e.g., voter, polling station, address, election) must be clearly identified at the business logic layer and encapsulated in 'business entity' components.

Identifier	Mandatory status	Description of requirement
NFR-AH.17	**M**	"Business entity" components must be cohesive and include all data and business logic related to their business entity, as needed to perform business operations, apply relevant business rules, and maintain the integrity and correctness of the data held.
NFR-AH.18	**M**	Components in the business logic layer must communicate with each other through dedicated internal interfaces/functions (tight coupling).
NFR-AH.19	**M**	The business logic layer components shall be accessible to external applications only through the external application interfaces defined for this purpose.
NFR-AH.20	**M**	The business logic layer architecture shall support concurrent access to system objects and functions.

Data model

The requirements regarding the data model are defined in Table 10.7:

Table 10.7. Requirements regarding the data model

Identifier	Mandatory status	Description of requirement
NFR-AH.21	**M**	The implemented and supported data model must take into account the current data architecture.
NFR-AH.22	**M**	The architecture of the data layer shall enforce the ACID rule (atomicity, consistency, isolation, durability) to guarantee data validity despite errors, interruptions, shutdowns, exceptions and other incidents.
NFR-AH.23	**M**	The IS shall ensure an integrated, unified data model for reference information (controlled lists, codes, addresses, polling stations, etc.), used consistently across all system modules and processes, with traceability, version control and interoperability with external systems.
NFR-AH.24	**M**	The SRV shall support creating, editing, processing, storing and accessing Unicode text.
NFR-AH.25	**M**	Data shall be accessible solely through the business logic layer components.
NFR-AH.26	**M**	Stored data shall be neutral and independent of the business logic layer.
NFR-AH.27	**M**	The data architecture shall be optimised to support rapid data access for executing transactions and for generating statistics and analytical reports. Generating analytical reports shall not affect the performance of the system's transactional operations.
NFR-AH.28	**M**	The implemented data model shall be documented in detail, including both the technical description (e.g. XSD, JSON Schema, UML) and the semantic description (associating data structures with business entities and their properties). The semantic documentation must be available to users with administrative rights within the system, where relevant (e.g. report configuration, rule definition).
NFR-AH.29	**M**	Each record related to an information object shall be assigned a unique identifier at system level. The algorithm for assigning the identification number shall be configurable within the system and shall enable the detection of record corruption.
NFR-AH.30	**M**	The system architecture shall ensure data integrity and correctness when multiple entities (users, internal processes, external applications) access and modify data simultaneously.
NFR-AH.31	**M**	Data shall be protected in proportion to their level of sensitivity. Security requirements shall be defined at data level (not at application level). This means that data security requirements should be set at the level of the

Identifier	Mandatory status	Description of requirement
		data themselves, thereafter serving as the basis for defining the security model applied at application and infrastructure levels. The security model applied at the level of data architecture shall ensure sufficient granularity to set access rights in accordance with legal regulations on data protection, including personal data.
NFR-AH.32	**M**	The CRUD matrix (Create, Read, Update, Delete) shall be used to present and validate the data access model. The Contractor shall submit the CRUD matrix for all categories of data and roles (business functions) related to the processes for managing and using the SRV.

Requirements regarding the technologies used

The technologies used for the SRV shall be compatible with virtualised environments and the existing infrastructure, be up to date (with no EOL components), and not impose artificial dependencies or unjustified additional services. The Contractor shall use current versions and ensure compatibility and long-term supportability. The requirements regarding the technologies used are set out in Table 10.8:

Table 10.8. Requirements regarding the technologies used

Identifier	Mandatory status	Description of requirement
NFR-TH.01	**M**	All system components (e.g., operating systems, middleware, databases) shall be capable of running in virtualised environments without restrictions.
NFR-TH.02	**D**	Where applicable, the use of the following recommended minimum technologies/solutions will be considered an advantage: • **Operating system (containers):** Minimal Linux distributions (e.g. Debian Slim), optimised for the Docker environment; • **Framework:** .NET 10 (cross-platform); • **ORM:** Entity Framework Core (EF Core); • **Dependency management:** NuGet; • **DBMS:** MS SQL Server 2022 (compatible with running in Linux containers) or equivalent open-source databases (e.g. PostgreSQL); • **Frontend:** A browser with support for ECMAScript 2025 (ES16) or higher, using a modern framework (e.g. Angular, React, Vue); • **Report generation:** Reporting solutions that can run in containers, or microservice-level document generation libraries, decoupled from the DBMS instance. Tenderers may propose equivalent technologies, provided they are fully compatible with a microservices-based architecture, can be packaged as OCI-compliant artefacts (lightweight Docker images), and do not mandate the use of Windows OS–based containers.
NFR-TH.03	**M**	The proposed architecture shall not introduce dependencies on external services or components that are not functionally justified and explicitly documented in the bid.
NFR-TH.04	**M**	The Contractor shall provide the latest versions and builds (including Cumulative Updates, Security Updates, Hotfix Updates) for all supplied components (except where there is a demonstrated incompatibility with components provided by the CEC).
NFR-TH.05	**M**	The Contractor shall not offer solutions that depend on obsolete or end-of-life technologies. All components shall have active support (LTS or equivalent) for at least three years from the date when the contract is signed.

Identifier	Mandatory status	Description of requirement
		All supplied and developed components shall be compatible and shall have no operational limitations on the latest versions of components available at the time (e.g. operating systems, DBMS, etc.).
NFR-TH.06	**M**	All public and interoperability APIs shall be defined using a spec-first approach and documented in OpenAPI 3.1 format; data models shall be delivered in JSON Schema format. The Supplier shall publish the OpenAPI specifications in a machine-readable format upon delivery. API contracts shall include request/response examples and error codes.
NFR-TH.07	**M**	Preferred technologies: Git (Gitea or self-hosted GitLab CE), OpenStack + Kubernetes for orchestration, NGINX for ingress/reverse proxy, PostgreSQL as the preferred relational database management system (RDBMS), MinIO for S3-compatible object storage, OpenSearch as the search engine, ClickHouse for columnar analytics, and RabbitMQ / Apache Kafka for messaging/streaming.

Interoperability requirements

The SRV shall ensure interoperability via interfaces using open, documented standards, for controlled integration with external systems (including through MConnect) and for exposing key business functions to other internal CEC systems. The data model and interoperability solutions must be documented and aligned with relevant best practices. Interoperability requirements are defined in Table 10.9:

Table 10.9. Interoperability requirements

Identifier	Mandatory status	Description of requirement
NFR-IO.01	**M**	All system interfaces shall be based on open standards. All message flows with external components shall be implemented using open standards.
NFR-IO.02	**M**	All provided interfaces shall be able to interact with external applications both in real time and in offline mode.
NFR-IO.03	**M**	The System shall include capabilities for defining new data exchange interfaces and adjusting the existing ones to access the system's business functions (e.g., document generation, transaction generation, accessing information on business entities).
NFR-IO.04	**M**	The System shall include capabilities for defining new interfaces to access external systems using open standards.
NFR-IO.05	**M**	The data model and interoperability solutions implemented in the Information System must be documented and aligned with European best practices (e.g., the ISA² programme and the European Interoperability Framework). The documentation will include both the technical description (e.g., XSD, JSON Schema, UML) and the semantic description (associating data structures to business entities and their properties). In addition, the IS shall take into account the following: - The SEMIC principles (Semantic Interoperability Community): using common vocabularies and standardised data models for entities such as persons, addresses, organisations and documents, to ensure semantic interoperability between registers and external systems. - The SDMX standard (Statistical Data and Metadata eXchange): applying standardised models and formats for the exchange of statistical data and metadata, particularly for electoral and statistical reporting, so that the data are compatible with national and European requirements.
NFR-IO.06	**M**	All system interfaces shall be properly documented (e.g., using the Web Services Description Language model).

Identifier	Mandatory status	Description of requirement
NFR-IO.07	**M**	Integration with the government interoperability platform MConnect is mandatory for data exchange flows with state entities. All endpoints intended for interoperability shall comply with OpenAPI contracts and shall be registered in the MConnect catalogue in accordance with AGE/STISC procedures.
NFR-IO.08	**M**	The System shall allow integration and interoperability with external systems using, alongside MConnect, other interaction types/interfaces (e.g., VMS/WFS[5]).

Performance requirements

The SRV shall ensure adequate operational performance (response time, concurrency, stability under load) and avoid degradation of transactional operation during resource-consuming processes (reports, analyses, imports). The Contractor shall describe the sizing parameters and the operating recommendations. The performance requirements are defined in Table 10.10:

Table 10.10. Performance requirements

Identifier	Mandatory status	Description of requirement
NFR-PF.01	**M**	The response time for a transactional user/service request provided by the system shall not exceed 2–3 seconds (except for report generation and the time required to extract data from other sources).
NFR-PF.02	**M**	The System shall be able to handle up to 300 concurrent sessions (from authorised users and external systems) without impact on performance, errors, or high use of resources.
NFR-PF.03	**M**	The Tenderer shall include in the system administration and operation guides information on processes that may reduce performance and its recommendations on running such processes concurrently (e.g., it is not recommended to run the process X for generating daily reports simultaneously with the process Y for exporting statistical data).
NFR-PF.04	**M**	Report generation and access to information for business analysis must not affect the system operational performance when processing transactions. The system documentation shall identify the reports with a significant impact on performance and set out the Contractor's recommendations for generating those reports so as not to affect performance indicators.
NFR-PF.05	**M**	The Tenderer shall specify in its bid the guaranteed minimum values for the system performance characteristics, referring to the technology platform recommended by the Tenderer and its configuration to operate in line with the stated/declared requirements (e.g., two DB servers connected via a Load Balancer).
NFR-PF.06	**I**	In line with the specific nature of the SRV, the system may require the import and processing of data on all citizens eligible to vote, as well as updates occurring in the SRP (overnight, daily).

Ergonomics and accessibility

The SRV interface shall be intuitive, ergonomic and accessible, allowing users to complete tasks with a minimal number of steps. The System shall comply with accessibility requirements (WCAG Level AA) and provide an appropriate experience across different resolutions and devices (particularly for functions for external users). The ergonomics and accessibility requirements are defined in Table 10.11:

Table 10.11. Ergonomics and accessibility requirements

[5] https://www.agcc.gov.md/content/informa%C8%9Bii-privind-monitorizarea-implement%C4%83rii-inds-0

Identifier	Mandatory status	Description of requirement
NFR-EA.01	**M**	All functions available to users shall be accessible via intuitive and informative graphical user interfaces.
NFR-EA.02	**M**	The user interface must ensure access to any relevant functionality through a minimal number of actions, optimised for simplicity and ergonomics. Navigation and execution of functions shall not involve unnecessary or redundant steps, and the UI structure shall comply with accessibility and usability principles in line with ISO 9241 and WCAG (Level AA) and shall follow the unified design model https://egov.md/ro/node/40993.
NFR-EA.03	**M**	User interface elements shall meet accessibility requirements in accordance with WCAG 2.0 Level AA, ensuring access to the system's functionality for users with various types of disabilities. This includes basic requirements (Level A) such as alternative text for images, keyboard navigation and a logical content order, as well as additional Level AA requirements, such as adequate visual contrast, clear navigation structures, compatibility with assistive technologies, and the ability to resize text without losing information.
NFR-EA.04	**M**	The user interface shall be optimised for desktop computers and notebooks, ensuring correct and ergonomic display at different screen resolutions. The System shall support at least the standard resolutions of 1920x1080 (FHD) and 2560x1440 (2K/QHD). The interface shall be adaptive, shall not lose functionality or legibility at these resolutions, and shall comply with ergonomics and accessibility principles in accordance with WCAG 2.0 Level AA.
NFR-EA.05	**M**	For functions available to external users (citizens), the System shall, for the most important functionalities, provide the ability to adapt the user interface according to the device used (notebook, desktop computer, tablet, smartphone).
NFR-EA.06	**M**	For mobile devices, interfaces adapted to the device type, operating system and resolution used shall be used. The System shall allow changing the displayed interface version (desktop/mobile) while keeping the user's session active.
NFR-EA.07	**M**	System users shall have access to context-sensitive help across all system interfaces.
NFR-EA.08	**M**	When using the report definition and configuration functions, users shall be able to access the data dictionary stored in the system.
NFR-EA.09	**M**	The Contractor shall take into account the SRV's current working practices and functionality to facilitate the user transition to the new system, while maintaining 85–90% of the existing menu structure, order, and business logic. All aspects of ergonomics, user interaction and business logic shall be agreed with the CEC and shall be accepted only after validation by the CEC.
NFR-EA.09	**M**	The frontend shall be implemented in TypeScript and shall adopt a mature component-based framework (e.g., React or Vue) in accordance with the Unified Design Model (MUD). Public portals shall support Server-Side Rendering (SSR) and comply with WCAG accessibility standards.

Security

The SRV shall be designed and implemented in line with Secure by Design principles, with documented security controls at all levels, minimum privileges, credential protection, and adherence to best practice (including prevention of OWASP Top 10 vulnerabilities). The requirements regarding security are set out in Table 10.12:

Table 10.12. Requirements regarding security

Identifier	Mandatory status	Description of requirement
NFR-SC.01	**M**	The architecture must be conceived by applying a "Secure by Design" approach.
NFR-SC.02	**M**	he system's security architecture shall be documented at all levels. The documentation shall describe the implemented security model, the included components, and the role of each component from a security perspective.
NFR-SC.03	**M**	All system processes related to the system components shall run with the minimum privileges necessary to perform their assigned tasks.
NFR-SC.04	**M**	The system shall not comprise, nor allow, the access credentials to be stored in plaintext within its components (in the database, configuration files, etc.).
NFR-SC.05	**M**	The system shall be designed and implemented according to security best practices, including prevention of vulnerabilities identified in the **OWASP Top 10**, and shall not contain or entail the use of software components with known security vulnerabilities or performance issues at the time of bid preparation. At the technical level, the submitted documentation shall include specifications concerning the network placement of the system components and the Contractor's recommendations regarding the network access rules to be configured by the CEC for secure access to all system components (e.g. inter-service communication matrix), for each of the system environments and for all nodes used.
NFR-SC.06	**M**	Authentication of citizens and identity integration shall be performed via MPass (OIDC/SAML) direct integration with individual QTSPs is not permitted.

Maintainability

The SRV shall be easy to administer, update and diagnose, so that daily operations and interventions (changes, fixes, extensions) can be carried out rapidly, in a controlled manner and with minimal risk. The requirements regarding maintainability are defined in Table 10.13:

Table 10.13. Requirements regarding maintainability

Identifier	Mandatory status	Description of requirement
NFR-MT.01	**M**	The Contractor shall deliver administration/operations documentation and runbooks, including installation, configuration, updating and troubleshooting, thus ensuring reproducible implementation (scripts/packages).
NFR-MT.02	**M**	The System shall ensure that configuration management is maintained separately from the code, is configurable per environment (dev/test/prod), and provides traceability of changes.
NFR-MT.03	**M**	The System shall ensure observability: standardised logging/audit, monitoring/health checks and alerts, without exposing sensitive data in logs.
NFR-MT.04	**M**	The Contractor shall ensure controlled update/upgrade (release notes, rollback), including a migration guide and version compatibility rules, where applicable.
NFR-MT.05	**M**	The System shall use unique error codes and controlled messages for users, with technical details in the logs.
NFR-MT.06	**M**	APIs shall be documented and versioned to prevent uncontrolled impact on external integrations.
NFR-MT.07	**I**	The Contractor shall deliver a minimum set of tests (unit/integration) and instructions for running them in the testing/training environment.

Identifier	Mandatory status	Description of requirement
NFR-MT.08	**I**	The Contractor shall train the administrators/operations staff and hand over training materials for future use.
NFR-MT.09	**M**	The Contractor shall provide backup/restore procedures and the steps for verifying restoration (restore test).

Scalability

The SRV shall be able to scale in a controlled manner (users, concurrent sessions, data volume and transaction volume) without significant performance degradation and without major architectural changes, and be compatible with operation in virtualised environments (including MCloud) and across two sites (HQ/DR). The requirements regarding the scalability are defined in Table 10.14:

Table 10.14. Requirements regarding the scalability

Identifier	Mandatory status	Description of requirement
NFR-SL.01	**M**	The System shall allow resource scaling (CPU/RAM/Storage) without restrictions imposed by the Contractor and without major architectural changes.
NFR-SL.02	**M**	The System shall handle an increase in the number of users/data volume and in concurrent sessions (e.g. 300), while maintaining response times within the performance requirements.
NFR-SL.03	**M**	The architecture shall allow layered scaling (presentation/logic/data), including horizontal scaling (adding nodes) and load balancing, where necessary.
NFR-SL.04	**M**	Batch/analytical tasks (bulk imports, reports) shall be designed so as not to significantly affect transactional operations; optimisations (e.g. caching/async) are permitted without compromising data integrity.
NFR-SL.05	**M**	The Contractor shall provide sizing recommendations, scaling limits/conditions and test scenarios (load/stress), with the indicators to be monitored to confirm scalability.
NFR-SL.06	**M**	Scaling and related configurations shall not introduce single points of failure (SPOF) and shall meet the resilience requirements.

11. Quality assurance process requirements

Purpose and general principles

The Contractor shall ensure a comprehensive testing and quality assurance (QA) process for the SRV, so that the delivered system complies with functional and non-functional requirements, is stable, secure and ready for operation, including during critical periods (election periods). Testing shall be planned, documented, repeatable and verifiable, with evidence presented to the CEC and the external QA team. The mandatory testing principles are defined in Table 11.1:

Table 11.1. General principles of testing and quality assurance

Identifier	Mandatory status	Description of requirement
CTQ.01	**M**	The Contractor shall ensure full traceability: each requirement (FR/NFR/UC) must be covered by one or more tests, with a mapping "Requirement → Test case → Result → Evidence".
CTQ.02	**M**	The System shall be separated into dedicated environments (at a minimum: development/test/pre-production & training), completely isolated from production.
CTQ.03	**M**	Testing in the production environment shall be performed only after full testing on other environments and the remediation of all defects that cause blockages or errors.
CTQ.04	**M**	Test sets (including regression) must be repeatable and executable at every release.
CTQ.05	**M**	Defects and errors shall be recorded, classified, remedied and re-tested, with full evidence of each defect's life-cycle.
CTQ.06	**M**	For each testing round there shall be evidence: logs, screenshots, reports, results of automated tests.
CTQ.07	**M**	The Contractor shall grant the Beneficiary and other parties designated by the Beneficiary for this purpose (external QA, EGA) full access to the testing documentation.

Test planning

The Contractor shall prepare the complete test planning documentation and submit it to the CEC and the external QA team for approval. The mandatory documents and associated requirements are defined in Table 11.2:

Table 11.2. Requirements regarding test planning

Identifier	Mandatory status	Description of requirement
CPQA.01	**M**	The Contractor shall develop and submit for approval to the CEC (and/or external QA) the Testing Strategy and Methodology, which shall include: the general approach, types of planned tests, acceptance criteria, team roles and responsibilities, and the tools used.
CPQA.02	**M**	The Contractor shall develop Test Plans that will contain: the activity schedule, the planned rounds with the objectives of each round, entry and exit conditions per round, allocated resources, identified risks, and actions taken.
CPQA.03	**M**	The Contractor shall suggest that the Beneficiary adjust and optimise the UC/FR and, if necessary, shall develop others required for operation as needed by the Beneficiary.
CPQA.04	**M**	The Contractor shall develop a complete set of test cases/scenarios that will include: the critical scenarios for the SRV (covering UC/FR, as well as any other functional requirements and usage scenarios identified and agreed during

Identifier	Mandatory status	Description of requirement
		implementation), necessary preconditions, detailed execution steps, necessary test data, expected results, and test prioritisation.
CPQA.05	**M**	The Contractor shall develop the Traceability Matrix showing minimum coverage for all critical UC/FR and NFR, with evidence of the connections between requirements and tests.
CPQA.06	**M**	The Contractor shall prepare reports of test results for each testing round, containing: an executive summary, identified defects, general status, team recommendations, and attached evidence.

Mandatory test types

Functional tests

The Contractor shall carry out a complete set of tests to validate the system's compliance with the functional requirements. The requirements regarding functional tests are defined in Table 11.3:

Table 11.3. Requirements regarding functional tests

Identifier	Mandatory status	Description of requirement
CQTF.01	**M**	The Contractor shall carry out unit tests with minimum coverage for critical components: validations, calculations, business rules, public API functions, business logic, edge cases and exceptions
CQTF.02	**M**	The Contractor shall carry out integration tests to verify: flows between SRV modules, integrations with external systems (SRP, SAISE, MConnect), error handling and transaction retries, validation of data flows, and testing of APIs and web services.
CQTF.03	**M**	The Contractor shall carry out system (end-to-end) tests executing complete scenarios for essential UCs, including checks for different roles, permission validation, complete flows and real-world usage scenarios
CQTF.04	**M**	The Contractor shall organise and facilitate UAT (User Acceptance Testing) with real users responsible for the domains in question. The UAT process can be combined with end-user training activities
CQTF.05	**M**	The Contractor shall maintain a mandatory minimum set of regression tests, to be run at each delivery, with at least 70% automation, to verify that existing functionality has not been affected. The mandatory minimum set shall include: • Registering a new voter with IDNP validation • Updating data for an existing voter • Automatic synchronization with SRP • Generating the electoral rolls • Citizen access to their data • Processing a request to change the constituency • Generating statistical reports and exporting data • User authentication and authorisation • Assigning/modifying roles • Audit trail for critical operations

Non-functional tests - Performance

The Contractor shall carry out performance tests to validate compliance with the non-functional requirements in Chapter 10.6. The minimum performance targets and testing requirements are defined in Table 11.4:

Table 11.4. Requirements regarding performance tests

Identifier	Mandatory status	Description of requirement
CQTP.01	**M**	The Contractor shall carry out performance tests in line with the following minimum targets: • Authentication: max 3s with MPass, max 2s without MPass (normal load) • Search by IDNP: max 2s (database with 3+ million records) • Generation of a list of 1,000 persons: max 10s (PDF/Excel format) • Complex statistical report: max 30s (up to 100,000 records) • Batch import from SRP: min 10,000 records/minute (overnight process)
CQTP.02	**M**	The Contractor shall carry out load/stress tests to verify: • Normal load: 50 concurrent users, response time <2s and 300 concurrent sessions <3s (95th percentile) • Peak load (pre-election): Stable support for 1,000 concurrent users, response time <7s, with no errors or exceptions. • Duration of tests: at least 2 hours with results maintained and without overloading components
CQTP.03	**M**	The Contractor shall carry out stress tests to identify the system's limits: • Support at least 1,500 simultaneous users without crashes • Controlled performance degradation (no total lock-up) • Automatic recovery within 5 minutes after removing the overload
CQTP.04	**D**	The Contractor shall carry out stability/endurance (soak) tests over extended periods (24–48 hours) to identify memory leaks, detect progressive degradation, and verify long-term stability

Non-functional tests - Resilience

The Contractor shall carry out resilience tests to validate the requirements in Chapter 12.2. The requirements regarding resilience testing are defined in Table 11.5:

Table 11.5. Requirements regarding resilience testing

Identifier	Mandatory status	Description of requirement
CQTR.01	**M**	The Contractor shall carry out reliability/resilience tests in line with Chapter 12.2, including: Load Balancing testing, checks of HA/cluster/failover mechanisms, backup/restore tests, simulation of primary server failure, recovery-from-backup testing, and verification of synchronisation between redundant servers

Security tests

The Contractor shall carry out security tests to validate compliance with the requirements in Chapter 10.8 and to identify vulnerabilities. The security testing process and related requirements are defined in Table 11.6:

Table 11.6. Requirements regarding security testing

Identifier	Mandatory status	Description of requirement
CQTS.01	**M**	The Contractor shall ensure configuration and hardening checks for all delivered components and for the components hosting them (OS, DBMS, etc.).
CQTS.02	**M**	The Contractor shall perform vulnerability scans for relevant components (application/infrastructure) in the testing environments, using standardised tools and scanning in line with the OWASP Top 10.
CQTS.03	**M**	The Contractor shall rank identified vulnerabilities by severity (Critical, High, Medium, Low), prepare a remediation plan for each, conduct re-testing to confirm remediation, and provide full documentation of the process.
CQTS.04	**M**	If CEC or the QA company carry out separate external penetration tests, the Contractor shall provide the necessary environments, supply test accounts, shall

		ensure access to logs, shall remedy applicable findings, and shall perform post-remediation re-testing.

Test data

The Contractor shall prepare, together with CEC, representative data sets for realistic validation of the system. The requirements regarding the test data are defined in Table 11.7:

Table 11.7. Requirements regarding test data

Identifier	Mandatory status	Description of requirement
CQTD.01	**M**	The Contractor, together with CEC, shall define and prepare relevant data sets for the SRV, preferably using depersonalised data, to cover normal and exceptional scenarios (duplicate data, incomplete data, edge cases, extreme values), in accordance with legal and data protection requirements (Law No. 195/2024, GDPR).
CQTD.02	**M**	The test/pre-production environments shall be populated with the necessary data and configured to reflect the production environment as closely as possible, to allow realistic validation of performance and behaviour.
CQTD.03	**M**	The Contractor shall ensure clear separation between environments (dev/test/pre-prod/prod).

Defect management

The Contractor shall implement a formal defect management process throughout the project. The requirements regarding the defect management process are defined in Table 11.8:

Table 11.8. Requirements regarding defect management

Identifier	Mandatory status	Description of requirement
CQMD.01	**M**	The Contractor shall use a formal defect management process based on a ticketing system, ensuring that each defect is recorded with a unique ID, detailed description, steps to reproduce, and evidence (screenshots, logs).
CQMD.02	**M**	The Contractor shall rank defects in accordance with Table 11.9 and shall observe the agreed resolution timeframes.
CQMD.03	**M**	The defect lifecycle shall include: identification and logging, classification (severity and priority), assignment to a developer, remediation, mandatory re-testing, closure with a reference to the version/build in which the fix was applied.
CQMD.04	**M**	Upon completion of an iteration, the Contractor shall provide periodic reporting on open/closed defects, trend analysis and risk identification, as well as a dashboard with quality metrics.

The classification of defect severity and the resolution terms are defined in Table 11.9.

Table 11.9. Defect severity classification

Severity	Description	Resolution time	Acceptance criteria
Critical	Non-functional system, data loss, security breach	24 hours	0 defects at Go-Live
Major	Major functionality affected, significant impact	3 days	Agreed/justified limits
Medium	Minor functionality; an alternative solution exists	1 week	Planned for the next release
Minor	Aesthetic issues; UI/UX improvements	2 weeks	Can be postponed

Acceptance criteria

Each testing round will have clear entry and exit criteria to ensure the quality of the process.

Entry criteria for testing

The requirements that must be met before starting a testing round are defined in Table 11.10:

Table 11.10. Entry criteria for testing

Identifier	Mandatory status	Description of requirement
CQAI.01	**M**	Stable and functional environment available
CQAI.02	**M**	Build delivered in accordance with the specifications
CQAI.03	**M**	Test cases approved by CEC and the QA company
CQAI.04	**M**	Test data prepared and loaded
CQAI.05	**M**	Testing team established and trained
CQAI.06	**M**	Technical documentation available

Test exit criteria

The requirements that must be met to successfully complete a testing round are defined in Table 11.11.

Table 11.11. Test exit criteria

Identifier	Mandatory status	Description of requirement
CQAE.01	**M**	All critical tests carried out as planned
CQAE.02	**M**	Critical defects = 0 (zero)
CQAE.03	**M**	Major defects within agreed/justified limits
CQAE.04	**M**	Success rate >95% for critical tests
CQAE.05	**M**	Test report submitted and approved by CEC/QA
CQAE.06	**M**	Complete evidence available
CQAE.07	**M**	Documentation updated

Test deliverables

The mandatory documents and reports to be delivered throughout the testing process are defined in Table 11.12:

Table 11.12. Test deliverables

Identifier	Mandatory status	Description of requirement
CQLT.01	**M**	Testing Strategy/Methodology (at project start)
CQLT.02	**M**	Test Plan (by rounds/milestones)
CQLT.03	**M**	A full set of test cases/scenarios
CQLT.04	**M**	Traceability matrix (critical UC/FR/NFR)
CQLT.05	**M**	Testing reports (per round) with evidence attached
CQLT.06	**M**	Defect log with updated status
CQLT.07	**M**	Code coverage reports (for unit tests)
CQLT.08	**M**	Vulnerability scanning reports (with remediations)
CQLT.09	**M**	Performance testing reports (with metrics)
CQLT.10	**M**	Final quality report before Go-Live, which will include: • Summary of compliance with the requirements • Test results by category • Minutes and UAT results • Identified remaining risks and necessary measures • Justified recommendation for production deployment • Minutes of final acceptance testing

12. Operational requirements

Migration and transition

The Contractor shall ensure the migration, verification, and controlled correction of data from the current systems to the new SRV, including user accounts, while maintaining data integrity, completeness, consistency, and traceability, as well as operational continuity. The migration process shall be planned and shall integrate reporting and monitoring activities.

The general migration principles are defined in Table 12.1:

Table 12.1. General principles of the data migration process

Identifier	Mandatory status	Description of requirement
CMG.01	**M**	The Contractor shall coordinate with the CEC on potential critical periods (e.g. elections, electoral campaigns, if any), as well as maintenance activities for the components involved in the migration. Based on these and taking into account the workload and the technological aspects, the Contractor shall develop the migration plan and coordinate it with the CEC
CMG.02	**M**	Any data transformation, mapping or loading shall be documented to allow tracking of the source and all changes made (full traceability).
CMG.03	**M**	As part of the data migration process, the Contractor shall be responsible for: • Defining the methodology for data migration and communicating it to stakeholders. • Developing, monitoring and adjusting the migration plan, where duly justified. • Providing the software tools for data migration. • Establishing the quality rules for preparing the data sets for migration and implementing them within the tools used in the process. • Mapping the data provided by the CEC to the data structures in the SRV • Establishing the data reconciliation criteria • Participating in data cleaning and reconciliation activities • Verifying and validating the quality of data sets for import • Importing the prepared data into the SRV and producing detailed reports on the import results. • Identifying exceptions and errors in the data import and addressing the causes of the deficiencies
CMG.04	**M**	The migrated data must comply with the validation rules and the constraints of the SRV data model. Quality issues identified in the source data shall be remedied before the actual migration.
CMG.05	**M**	All migration activities shall be carried out securely: controlled access, extended event logging, and personal data protection in accordance with the GDPR and legislation in force.
CMG.06	**M**	A rollback mechanism shall be in place in the event of a migration failure, allowing a return to the previous state.
CMG.07	**M**	The final list of sources and the precise volumetrics shall be established within the first four weeks of the project, following a detailed inventory.

Data sources and volumetrics

The data sources for migration and the estimated volumetrics are presented in Table 12.2:

Table 12.2. Data sources and estimated volumetrics.

Source	Data categories	Estimated volumetrics
Current SRV	Data on voters: IDNP, personal information, addresses, status, change history Polling stations: current and past configurations	~3,000,000 voters ~500,000 unique addresses

Source	Data categories	Estimated volumetrics
	Assignments of voters to polling stations per election Declarations of residence Controlled lists and classification catalogues Users, roles, access rights	~2,000 active polling stations + history Variable volumes
SAISE TechDB	Electoral rolls from previous elections Polling station configurations per election Data on voter turnout SAISE controlled lists	The last 3-5 elections
Other sources	Shall be defined as part of the migration process	Confirmed during the analysis phase

Mandatory activities of the Contractor

A) Analysis and inventory of current data

The Contractor shall carry out a detailed analysis of all existing data sources. The requirements regarding the analysis and inventory are defined in Table 12.3:

Table 12.3. Requirements regarding analysis and data inventory

Identifier	Mandatory status	Description of requirement
CAI.01	**M**	The Contractor shall document the current data structures: tables, relationships, types, etc.
CAI.02	**M**	The Contractor shall determine the exact volumetrics for all data sources, as required for the migration
CAI.03	**M**	The Contractor shall identify quality issues: duplicate records, missing or incomplete data, inconsistencies between sources, non-standard formats, invalid values
CAI.04	**M**	The Contractor shall coordinate with CEC on the methodology for inventory, analysis and data quality assessment.
CAI.05	**M**	The Contractor shall propose a data cleansing strategy based on the analysis performed.
CAI.06	**M**	The Contractor shall confirm with CEC the final list of datasets for migration.
CAI.07	**M**	The Contractor shall confirm with CEC the source of truth for each data category (e.g., for voters' personal data, the primary source is SRP).
CAI.08	**M**	The Contractor shall deliver the current data analysis report and a source inventory, including quality assessment and appropriate recommendations for remediation.

B) Data planning and cleansing

The Contractor shall develop a detailed migration plan and implement data cleaning mechanisms. The requirements are defined in Table 12.4:

Table 12.4. Requirements regarding data planning and cleansing

Identifier	Mandatory status	Description of requirement
CPC.01	**M**	The Contractor shall develop a detailed migration plan to be submitted for CEC approval
CPC.02	**M**	The plan shall include the migration strategy: phased implementation, a mandatory pilot migration on a sample, ahead of the complete migration
CPC.03	**M**	The plan shall include detailed mapping of the data from the source system to the new SRV data model (field by field).
CPC.04	**M**	The plan shall include the transformation and normalisation rules, handling erroneous or incomplete data, deduplication, and conflict resolution.

Identifier	Mandatory status	Description of requirement
CPC.05	**M**	The Contractor shall deliver automated scripts for data cleaning: removing duplicates, standardising formats (addresses, dates, IDNP), validation against official controlled lists, and filling in missing data.
CPC.06	**M**	Before any operation, the Contractor shall conduct a full backup of all source databases and validate it by test restoration.

C) Pilot migration - mandatory

Before the full migration, the Contractor shall conduct a pilot migration on a representative subset. The requirements regarding the pilot migration are defined in Table 12.5:

Table 12.5. Requirements regarding the pilot migration

Identifier	Mandatory status	Description of requirement
CMP.01	**M**	The Contractor shall perform a pilot migration on a full set of voters that includes all types of data: active and inactive voters, declarations of residence, urban and rural polling stations, local controlled lists, etc.
CMP.02	**M**	The pilot migration shall be considered successful only if: all automated validations pass at 100%, manual sampling is 100% correct, CEC users confirm data correctness and functionality, and the extrapolated execution time does not exceed 48 hours.
CMP.03	**M**	Should the validations fail, the Contractor shall remedy the issues and rerun the pilot

D) Validation, stabilisation and acceptance

The requirements for ensuring post-migration validation and system stabilisation are defined in Table 12.6:

Table 12.6. Requirements for validation, stabilisation and acceptance

Identifier	Mandatory status	Description of requirement
CVA.01	**M**	The Contractor shall carry out comprehensive post-migration validation, including completeness checks (number of records, data sets), consistency and integrity checks (model constraints, valid references, unique keys, controlled lists), and reconciliations on samples and critical sets
CVA.02	**M**	The Contractor shall perform functional confirmation through key scenarios: search by IDNP, voter profile display, electoral roll generation, export of voter lists to SAISE (e_Day) – performed together with CEC users and external QA
CVA.03	**M**	In the first 30 days after the full migration, the Contractor shall monitor and ensure performance improvements
CVA.04	**M**	The Contractor shall train the CEC teams in data operations: regular SRP imports, manual corrections, and reconciliation procedures
CVA.05	**M**	The Contractor shall hand over the migration artefacts (ETL scripts, mappings, procedures, checklists) with full documentation necessary for efficient operation
CVA.06	**M**	Acceptance criterion – Zero data loss: 100% migrated (automatic count reconciliation)
CVA.07	**M**	Acceptance criterion – Referential integrity: 100% (automated validations, zero orphan references)
CVA.08	**M**	The migration shall be considered accepted when every criterion has been met and the acceptance document is signed by the CEC.

Resilience and continuity

The Contractor shall design and configure the SRV to ensure service continuity and resilience against incidents — hardware or software failures, configuration errors, network outages, unavailable components, and degraded performance. The solution shall minimise single points of failure and support rapid service restoration following disruptive incidents.

The Contractor shall implement a High Availability (HA) architecture with cluster configuration for the system's critical components. The unavailability of one instance shall not result in a complete service disruption — other instances in the cluster shall automatically take over the traffic (automatic failover). The requirements for HA architecture are defined in Table 12.7. Requirements for High Availability architecture:

Table 12.7. Requirements for High Availability architecture

Identifier	Mandatory status	Description of requirement
CHA.01	**M**	
CHA.02	**M**	The System shall have mechanisms ensuring data integrity in the event of accidental failures affecting any of its components.
CHA.03	**M**	The System shall include mechanisms to quickly restore the availability and accessibility in the event of continuity incidents.
CHA.04	**M**	The Contractor shall implement cluster configurations for critical components: application servers, databases, integration components with external systems (SRP, SAISE, MConnect), and authentication services
CHA.05	**M**	The Contractor shall implement load balancing for web traffic with at least two active application servers
CHA.06	**M**	The Contractor shall configure databases in a primary–standby setup with synchronous or asynchronous replication (defined RPO)
CHA.07	**D**	The Contractor shall implement automated health checks and automatic restarts for failed services
CHA.08	**D**	The Contractor shall ensure session persistence to prevent loss of user sessions during failures
CHA.09	**M**	The Contractor shall document in detail the redundancy and failover mechanisms
CHA.10	**M**	The Contractor shall implement a monitoring system that rapidly detects degradations and initiates automated interventions or alerts the operations team
CHA.11	**M**	The Contractor shall validate the redundancy and failover mechanisms through testing

Note: The detailed documentation concerning the resilience mechanisms shall be delivered in accordance with Chapter 13.2 (Requirements for documentation). Training for the CEC teams on resilience and continuity procedures shall be carried out in line with Chapter 12.3 (Training and knowledge transfer).

Training and knowledge transfer

The Contractor shall provide training to all categories of SRV users prior to Go-Live, in accordance with each group's roles and responsibilities. The aim of the training is to ensure full operational autonomy of the CEC and its institutional partners in the use, administration and maintenance of the SRV, without dependence on the Contractor following contract expiry.

General requirements for the Training Plan

The general requirements for the Training Plan are set out in Table 12.8. General requirements for the Training Plan:

Table 12.8. General requirements for the Training Plan

Identifier	Mandatory status	Description Requirement

CTRN.01	**M**	The Contractor shall develop and submit for approval a detailed Training Plan at least 15 days prior to the user acceptance testing (UAT) phase. The Plan shall include the schedule, the modules covered, and the format of the sessions (on-site or online).
CTRN.02	**M**	All practical training sessions shall be conducted exclusively in a Test/Staging environment (an exact replica of the production environment), and the use of the production environment for simulations or the creation of dummy data is strictly prohibited.
CTRN.03	**M**	The data used for training shall be masked or cleansed so as not to pose a risk of unauthorised access to personal data.

Specific requirements per user group

The Contractor shall tailor the content and format of the training sessions to the profile of each group, as follows:

Group 1 – IT Staff (Administration, Management and Support)

The training requirements for technical staff are set out in Table 12.9:

Table 12.9. Group 1: IT Staff (Administration, Management and Support)

Identifier	Mandatory status	Description Requirement
CTRN.04	**M**	The sessions for the technical team shall cover Docker container management, microservices monitoring, deployment of updates (CI/CD), and the management of artefacts in the internal registry.
CTRN.05	**M**	The knowledge transfer shall ensure that IT staff are fully prepared to independently assume first- and second-line support in incident management. This includes diagnostic procedures using *Correlation IDs*, log interpretation, and other maintenance activities.
CTRN.06	**M**	The Contractor shall ensure the transfer of theoretical and practical knowledge to CEC representatives, necessary for the administration, maintenance, and management of the microservices and container infrastructure. To this end, training sessions shall be conducted, and educational materials, instructions, guides, and any other necessary documentation shall be provided.

Group 2 – CEC Employees with Business/Management Roles

This group uses the SRV for daily operations, decision-making, and report generation. The sessions focus on understanding operational workflows and business logic. The requirements are set out in Table 12.10:

Table 12.10. Group 2: Employees (Business/Management Roles)

Identifier	Mandatory status	Description Requirement
CTRN.07	**M**	The sessions for employees with complex roles shall focus on business logic, approvals, report generation, task delegation, and the interpretation of aggregated data in dashboard interfaces.
CTRN.08	**M**	**"Train the Trainer" sessions (Optional/Desirable):** The Contractor shall train a small group of key employees to acquire the skills necessary to subsequently train other new colleagues within the institution.

Group 3 - Registrars

Registrars constitute the largest group of SRV users and are geographically distributed across municipal town halls and CEC district offices. Training for this group is practical and operational in nature. The requirements are set out in Table 12.11.

Table 12.11. Group 3: Registrars

Identifier	Mandatory status	Description Requirement
CTRN.09	**M**	**Basic Operational Training:** The training shall be conducted exclusively on the registration interface, focusing on rapid navigation, accurate data entry, validation of data and forms, and the use of keyboard shortcuts (where applicable).

Group 4 - External users (Voter, Visitor)

External users access the SRV via the public interface without face-to-face training sessions. The Contractor shall ensure the necessary informational support in accordance with the requirements set out in Table 12.12.

Table 12.12. Group 4 - External users

Identifier	Mandatory status	Description of requirement
CTRN.10	**M**	The Contractor shall deliver online user guides (FAQs, step-by-step tutorials) for publicly accessible functionalities: data verification, declaration of residence, and public interface navigation. These form part of the CDG.05 deliverables.

Note: *Training of the CEC teams shall also include aspects related to resilience and continuity. Training sessions shall be conducted taking into account the operational requirements of users, as well as CDG.05 (user documentation). The materials developed within the training activities shall form part of the project's documentation deliverables.*

13. Requirements for project management

The Contractor shall demonstrate the maturity of the practices applied in implementing the SRV by presenting relevant certificates of conformity and examples of similar projects implemented, both at company level and by team members. The Contractor shall also refer to and provide a detailed explanation of the methodological approach for both project management and the specific development and implementation activities at all stages of the project.

Table 13.1. General requirements for project management

Identifier	Mandatory status	Description of requirement
PMG.01	**M**	The Contractor has primary responsibility for project management in accordance with the methodology proposed and agreed with the Beneficiary. The Contractor is responsible for identifying and mobilising the resources required to perform the activities within its area of responsibility, as set out in the project management plan, at the agreed quality level.
PMG.02	**M**	The Contractor shall have at least one person (PM) dedicated to project management.
PMG.03	**I**	The Beneficiary is responsible for all procedures and administrative aspects related to the implementation of the project, including the organisation of the internal project team and the preparation of the ICT environment necessary for the implementation of the SRV.
PMG.04	**I**	The CEC shall appoint a project manager who will manage the Beneficiary's project teams.
PMG.05	**I**	The entire implementation process will be overseen and monitored by several parties (in addition to the Beneficiary and the Contractor), who will be involved at all stages, each delegating a project manager, comprising permanent members and invited participants as required. - UNDP (on a permanent basis), - QA – a company responsible for providing project monitoring and control services (on a permanent basis), - STISC (invited) - e-Governance Agency (invited).
PMG.06	**M**	The project is to be delivered using a hybrid approach that combines elements of the Waterfall methodology with techniques from the Agile methodology. In light of the above, the Tenderer shall propose an implementation methodology, accompanied by a detailed description of the project approach, demonstrating how the project will be implemented and its objectives achieved. The detailed requirements for the development process are set out in Table 13.2. SRV development process requirements.
PMG.07	**M**	The Contractor is responsible for the quality of the project deliverables. If the deliverables contain defects not attributable to the Beneficiary, the Contractor shall rectify them without any changes to the schedule, project timelines, or costs, including during the warranty period.
PMG.08	**M**	The Contractor is responsible for finalising or updating and submitting, on a monthly basis unless otherwise agreed with the Beneficiary, the results/deliverables in accordance with the plan, as well as reports related to the project management process and the project registers.
PMG.09	**M**	All communication and deliverables within project management activities shall be in Romanian.
PMG.10	**M**	The Tenderer shall include in its offer a draft project management plan (Project Charter). The document shall describe at least the following:

Identifier	Mandatory status	Description of requirement
		• Project context, which shall include: Purpose and objectives, scope (what is included in and excluded from the project), Beneficiaries, Stakeholders, and deliverables; • The project management organigramme, including: the project steering committee, the roles of the Contractor's project team members, the roles of the Beneficiary's project team members, UNDP and other parties (PMG.05). For each role, the key responsibilities within the project shall be defined (RACI matrix); • The initial version of the Project Plan (WBS), describing the timeframes and the content of the product versions to be delivered; • The communication plan, including: communication methods, communication channels, frequency of communication (what, when, how, to whom), responsibilities, escalation mechanisms, confidentiality rules, procedures, and special situations. • Practices applied to interaction and collaboration within the project, including: management of the project plan, detailed planning of activities based on prioritised requirements, resource management, change management, risk management, quality management of deliverables, progress monitoring and reporting, exception management, and management of the Project Library. • Risk management: a template for the RAID log, a description of potential risks, risk management strategies, and mitigation (treatment) actions; • Quality management: Quality assurance procedures; • Change management strategy, including: Procedures for change control and approval, setting out how changes within the project will be managed and approved, and who is responsible for their approval; • The list and templates for the project registers proposed by the Tenderer.
PMG.11	**M**	After signing the Contract with the Contractor, the Contractor shall submit an updated, more detailed and accurate version of the Project Management Plan (Project Charter), adapted and updated to take into account all necessary data about the Beneficiary and the applicable technical, managerial and logistical aspects. In the expanded version, the Contractor shall present in detail the methodology for all project activities, where applicable, and at a minimum for: • Code development, component development, and implementation; • Testing and quality assurance; • Security and resilience; • Other items mentioned (service requests, incidents, etc.).
PMG.12	**M**	It is expected that at least the following project registers will be maintained: 1. RACI Matrix for each stage of the project; 2. Communications and meetings register; 3. Cases (service, support, incidents, requests, etc.); 4. Change register; 5. Risk register (RAID Log); 6. Version register; 7. Test results register; 8. Lessons learned.

The project is to be delivered using a hybrid approach that combines elements of the Waterfall methodology with techniques from the Agile methodology. In light of the above, the Tenderer shall propose an implementation methodology, accompanied by a detailed description of the project approach, demonstrating

how the project will be implemented and its objectives achieved. The detailed requirements for the development process are set out in Table 13.2. SRV development process requirements.

Table 13.2. SRV development process requirements

Identifier	Mandatory status	Description of requirement
CDEV.01	**M**	The SRV is to be designed and developed using a hybrid project management approach. In this context, the Contractor shall carry out a business analysis (specific to the Waterfall approach) prior to the start of the SRV design and development phase. Based on the results of the business analysis, the Project Backlog shall be developed and shall thereafter be used in the SRV development iterations.
CDEV.02	**M**	The SRV design and development shall be carried out using an Agile approach to project management (the information system shall be designed and developed in an iterative and incremental manner, applying CI/CD practices (continuous integration and continuous delivery)).
CDEV.03	**M**	The length of each iteration (project sprint) during the SRV development phase shall be two weeks. Depending on the progress of development, the duration may, if necessary, be increased to three weeks.
CDEV.04	**M**	During each sprint, the Contractor shall perform the following activities: · selecting relevant tasks from the Project Backlog for implementation within the sprint (or carrying over incomplete tasks from the previous sprint); · conducting business analysis for the Project Backlog tasks to be implemented within the sprint; · preparing user stories for the Project Backlog tasks selected for implementation within the sprint; · developing the functionalities planned for the sprint; · internally testing the functionalities implemented within the sprint; · preparing and updating the technical documentation for the functionalities implemented within the sprint (for example: the System Design Document (SDD), guides, specific procedures, etc.); · updating the Project Backlog (where necessary).
CDEV.05	**M**	For development activities, the Contractor shall prepare periodic (per-sprint) project management reports to succinctly inform the project stakeholders about: · completed tasks; · tasks to be completed in the next period; · tasks planned for the next period; · issues and questions related to current activities; · current risks and mitigation measures.
CDEV.06	**M**	The Contractor shall periodically conduct demonstrations of the implemented functionalities and collect comments and suggestions from project stakeholders for consideration in the SRV development process.
CDEV.07	**M**	The Contractor shall be able to deploy specific SRV functionalities into production, if necessary (project stakeholders may decide on the functional modules to be put into production before the development phase is fully completed).

Requirements regarding the microservices-based architecture

General requirements

At the project initiation stage, the Contractor shall, in collaboration with the Beneficiary, define the approach for developing the RSV based on microservices, as well as the feasibility and methods of integration with the Government Git platform.

Table 13.3. Requirements for microservices

Identifier	Mandatory status	Description Requirement
CDK.01	**M**	The SRV shall be developed using a container-based architecture. The System shall be designed in a modular manner, with each component (frontend, backend, databases, services) running in separate Docker containers.
CDK.02	**M**	The delivered Docker images shall comply with Open Container Initiative (OCI) standards to ensure interoperability.
CDK.03	**M**	Minimalist base images (lightweight base images, e.g., Alpine, Debian Slim) shall be used to reduce the size of artefacts and the number of vulnerabilities.
CDK.04	**M**	The application shall comply with the stateless design principle. Storing persistent data or sessions inside the container is strictly prohibited. Any state (file storage, sessions) shall be managed via external volumes or database services and not within the container.
CDK.05	**M**	The Contractor shall deliver Docker Compose (docker-compose.yml) files for the development, testing and pre-production environments, which allow the entire service stack to be brought up in an orchestrated manner.
CDK.06	**M**	All environment-specific settings (credentials, IP addresses, API keys, etc.) shall be injected exclusively via environment variables or .env files, not hard-coded.
CDK.07	**M**	Restart Policies: Containers shall be configured with automatic restart policies (e.g. unless-stopped) to ensure service availability upon host reboot (and in the event of failure).
CDK.08	**M**	Persistent data (databases, logs, uploaded files) shall be mapped to external volumes or directories mounted from the host.
CDK.09	**M**	Specific virtual Docker networks (e.g. frontend_net, backend_net, db_net) shall be defined to isolate traffic and restrict direct access to the database from external sources.
CDK.10	**M**	Processes in containers shall not run as the root user. The Dockerfile shall specify a user with the minimum necessary privileges.
CDK.11	**M**	Sensitive information shall not be included in container images. Securely mounted volumes or Docker Secrets-type mechanisms shall be used.
CDK.12	**D**	The Contractor shall submit an image scanning report (e.g., using Trivy or Grype) confirming the absence of critical vulnerabilities.
CDK.13	**M**	The Contractor shall assist the Beneficiary in configuring a storage environment (Registry) for the final Docker images within the Beneficiary's own infrastructure.
CDK.14	**M**	The deliverables shall include clear procedures for building, updating, volume backups and container monitoring.
CDK.15	**M**	The Contractor shall organise training sessions for the Beneficiary's technical team on the administration of the containerised solution.
CDK.16	**M**	The System shall be compatible with advanced orchestrators (Kubernetes or Docker Swarm) to enable subsequent scaling.
CDK.17	**M**	All application logs shall be sent to STDOUT/STDERR to be collected natively by Docker's logging mechanism.

The Contractor shall ensure the implementation of a microservices architecture based on a CI/CD pipeline (Continuous Integration / Continuous Deployment). The requirements regarding the CI/CD pipeline are set out in Table 13.4:

Table 13.4. Requirements for the CI/CD pipeline

Identifier	Mandatory status	Description Requirement
CCI.01	**M**	The Contractor shall ensure that the entire process of installing and configuring the microservices architecture from scratch on the Beneficiary's infrastructure is carried out. To this end, the Contractor shall provide support to the Beneficiary in the configuration and/or provisioning of the necessary resources, as well as in the adjustment of the infrastructure required for system operation. The specific requirements for resources, environments, and support services shall be defined and coordinated with the Beneficiary during the project planning stage.
CCI.02	**M**	Source Code Versioning: All source code, including Docker configuration files (Dockerfile, docker-compose.yml), shall be managed in a version control system (e.g., Git).
CCI.03	**M**	Automated Build: Any change (commit) to the main branch (main/master) shall automatically trigger the build of a new Docker image.
CCI.04	**M**	In-Container Testing: The CI pipeline shall include a stage that automatically runs tests (unit tests, integration tests) within a dedicated container before the image is validated.
CCI.05	**M**	Versioning (Tagging): Images shall not use the generic "latest" tag in production. Each build shall generate a unique tag (e.g., based on the Git hash or the semantic version v1.2.3).
CCI.06	**M**	Security Scan (Pipeline): Integration of an automated image scanning stage for vulnerabilities before it is pushed to the registry. The build shall not be accepted if "Critical" vulnerabilities are identified.
CCI.07	**M**	Image Promotion: The same image (artifact) that was tested in the Test environment shall also be used in the Production environment, without a rebuild (the *Build Once, Run Anywhere* principle).
CCI.08	**D**	Automated Deployment (CD): The System shall allow the automatic update of containers on the test server as soon as the build is successfully completed.
CCI.09	**M**	Rollback Procedure: The Contractor shall demonstrate and document the procedure for reverting a container to a previous version in under 5 minutes in the event of a major error.
CCI.10	**M**	Environment Isolation: The delivery pipeline shall ensure strict separation of configuration variables (secrets) between the Development, Test, Pre-Prod, and Production environments.
CCI.11	**M**	Notifications: The CI/CD system shall notify administrators (via email or a messaging system) of the success or failure of each build/deploy process.

The Contractor shall ensure the installation and configuration of the tools required for CI/CD on the Beneficiary's infrastructure. Requirements for administering the CI/CD environment are set out in Table 13.5.

Table 13.5. Requirements for the administration of the CI/CD environment

Identifier	Mandatory status	Description Requirement
CADM.01	**M**	CI/CD Environment & Registry Configuration: The Contractor shall ensure the installation and configuration of a CI/CD server (e.g. GitLab Runner, Jenkins) and a private Docker image registry (e.g. Harbor, Nexus) within the institution's infrastructure.
CADM.02	**M**	Backup of the Image Registry: The Contractor shall implement an automated backup procedure for Docker images stored in the private registry, ensuring the redundancy of production artefacts on a separate storage medium.
CADM.03	**M**	Backup of Source Code (Git): The Contractor shall configure periodic backups for the source code repository (including commit history and deployment configurations), stored outside the primary development server.
CADM.04	**M**	Disaster Recovery (Platform): The Contractor shall deliver a disaster recovery plan describing the complete reconstruction of the Docker platform (including networks, volumes and containers) from scratch, using exclusively the existing backups.
CADM.05	**M**	Full Transfer of Access: Upon completion of the project, the Contractor shall transfer all administrator accounts, encryption keys, access tokens and passwords required for the autonomous management of the entire Docker and CI/CD infrastructure.
CADM.06	**M**	Image Maintenance (Patching): During the warranty period, the Contractor shall update (rebuild) the Docker images whenever security vulnerabilities are identified in the base libraries (OS-level patching).
CADM.07	**D**	Resource Monitoring: The Contractor shall ensure the implementation of a monitoring dashboard (e.g. Portainer or Grafana) enabling the CEC IT team to view container status, RAM and CPU usage, and logs in real time.
CADM.08	**M**	The Contractor shall ensure the integration of the delivered components with the institution's internal services (e.g. AD, SIEM), as required.

Source Code Delivery, Traceability and Documentation

The requirements for the quality, documentation and delivery method of the source code to the Beneficiary are set out in Table 13.6:

Table 13.6. Requirements regarding source code delivery

Identifier	Mandatory status	Description Requirement
CSRC.01	**M**	**Delivery via Version Control System (Git):** The source code shall not be delivered as a static archive, but through the full transfer of the Git repositories. They shall contain the complete history of commits, branches and tags from the start of the project through to acceptance.
CSRC.02	**M**	**Open and Unobfuscated Code:** All specifically developed source code shall be delivered in plain text format. The use of obfuscation techniques or the compilation of business logic into opaque binary libraries (black-box) shall be

Identifier	Mandatory status	Description Requirement
		strictly prohibited, except for standard commercial off-the-shelf (COTS) products agreed in advance.
CSRC.03	**M**	**Traceability from Code to Artefact:** The Tenderer shall precisely document the correspondence between a specific *tag* in the Git repository and the **artefact** (Docker image) deployed in the production environment at the time of acceptance.
CSRC.04	**M**	**Commenting Complex Logic:** Functions, procedures, classes and complex algorithms shall be accompanied by explanatory *inline* comments. The code shall use recognised standards for documenting code blocks (e.g. JavaDoc, PHPDoc, JSDoc, Docstrings), specifying the input parameters, the return data type, and any exceptions that may be thrown.
CSRC.05	**M**	**Documentation of Custom Libraries:** Any code library (library/package) developed by the Contractor for reuse across multiple microservices (e.g. an internal logging or parsing package) shall be treated as a standalone product. It shall have its own detailed README.md, including import and usage instructions.
CSRC.06	**M**	**Clean Code:** The naming of variables, methods and classes shall be self-descriptive, in English, reflecting the intended purpose and business domain.
CSRC.07	**D**	**Architecture Decision Record:** For any atypical implementation or major architectural decision reflected in the code, an *Architecture Decision Record* (ADR) file shall be created in the repository, explaining why that approach was chosen over alternative options.
CSRC.08	**M**	**Dependency List:** Each code component shall include package management files (e.g. package.json, requirements.txt, pom.xml, go.mod) that explicitly list all external dependencies (third-party libraries). The versions of these packages shall be pinned to ensure build reproducibility.
CSRC.09	**M**	**Third-Party Licence Audit:** The Tenderer shall deliver a centralised report of all open-source libraries used and their licence types (MIT, Apache 2.0, BSD, etc.). The inclusion of 'viral' licensed libraries (e.g. GPL v3) in the application code shall be strictly prohibited, as such inclusion would require the Institution to publish the entire system source code free of charge, without the Beneficiary's prior written consent.
CSRC.10	**M**	**Local Build Guide:** The source code shall be accompanied by technical documentation detailing the exact steps (terminal commands) required to compile the source code and rebuild the Docker images from scratch on a freshly installed workstation, independent of the Contractor's CI/CD environment.
CSRC.11	**M**	**Technical deliverables:** OpenAPI 3.1 files for public APIs; JSON Schema for data models; source code in a Git repository (Gitea/GitLab CE compatible); Dockerfiles/OCI images for components; IaC instructions (Ansible / OpenTofu) for environment provisioning; integration documentation for MPass, MConnect, MLog, and other internal CEC and governmental services.

Security Requirements in Relation to the Development Process

The requirements regarding the security of the development, deployment and operation of microservices and containers are set out in Table 13.7.

Table 13.7. Security requirements for microservices and containers

Identifier	Mandatory status	Description Requirement
CSDV.01	**M**	**Read-Only File System:** All containers shall run with a strictly read-only root filesystem. Any required write operations (e.g. temporary files, cache) shall be performed exclusively within dedicated temporary volumes (tmpfs).
CSDV.02	**M**	**Resource Limits (cgroups):** To prevent DoS (Denial of Service) attacks targeting the exhaustion of host resources, each container shall have strict hard limits configured for CPU and RAM usage.
CSDV.03	**M**	**Minimal Kernel Privileges (Drop Capabilities):** Containers shall be configured to drop all unnecessary Linux kernel capabilities (cap-drop=ALL), retaining only those strictly required for the application to operate. No container shall be run in privileged mode (--privileged).
CSDV.04	**M**	**Digitally Signed Images (Content Trust):** The system shall only allow the execution of artefacts (Docker images) that have been digitally signed by the authorised CI/CD pipeline, thereby preventing the injection of malicious images.
CSDV.05	**M**	**Encryption of Internal Traffic (mTLS):** All data communication between microservices on the internal network shall be encrypted and mutually authenticated using mutual TLS (mTLS). Plaintext internal traffic (plain HTTP) shall not be permitted.
CSDV.06	**M**	**API Gateway as the Single Point of Entry:** All external traffic shall be routed through an API Gateway, which shall act as a security barrier, enforcing rate limiting to prevent brute-force attacks.
CSDV.07	**M**	**WAF Protection (Web Application Firewall):** The API Gateway or Load Balancer shall be integrated with a WAF solution capable of inspecting traffic and proactively blocking attacks from the OWASP Top 10 (e.g. SQL Injection, Cross-Site Scripting).
CSDV.08	**M**	**Network Segmentation (Network Policies):** Strict firewall rules shall be implemented at the Docker/Orchestrator virtual network level, allowing communication only between microservices that legitimately require it (default deny).
CSDV.09	**M**	**Centralised and Stateless Authentication:** The System shall use a centralised Identity Provider (IdP) (e.g. Keycloak) and standard protocols (OAuth 2.0 / OpenID Connect). Sessions shall not be stored in memory; authorisation shall be performed by validating the signature of JWT tokens (JSON Web Tokens).
CSDV.10	**M**	**Token Validation at Service Level:** Each microservice shall independently validate the signature, validity period and permissions (claims/scopes) of the JWT token for every incoming request, in accordance with the Zero Trust principle.
CSDV.11	**M**	**Masking of Sensitive Data (Data Masking/Sanitisation):** Any log or error message returned by microservices shall be automatically sanitised to ensure that PII (Personally Identifiable Information), passwords, tokens or internal database structures are never exposed.
CSDV.12	**M**	**Data-at-Rest Encryption:** All persistent storage volumes associated with databases and file storage systems shall be encrypted using industry-standard algorithms (e.g. AES-256).
CSDV.13	**M**	**Component Transparency (SBOM):** At each new version release, the Tenderer shall generate and deliver an SBOM (Software Bill of Materials) for each **artefact**,

Identifier	Mandatory status	Description Requirement
		enabling the Institution to maintain full traceability of all internal and external libraries used.
CSDV.14	**M**	**Preventing Hard-Coding of Secrets:** The delivery pipeline (CI/CD) shall include a source code scanning stage to automatically block any commit containing potential hard-coded passwords, API keys or certificates (e.g. using tools such as *TruffleHog* or *Gitleaks*).

Requirements for documentation

The Contractor shall develop and submit to UNDP and CEC (the Beneficiary) documentation relating to the State Register of Voters. The documents shall be coordinated and approved by UNDP and the Beneficiary. The general requirements for the delivered documents are set out in Table 13.8:

Table 13.8. General requirements for the documents delivered by the Contractor

Identifier	Mandatory status	Description of requirement
CDG.01	**M**	The Contractor shall ensure the proper record-keeping and quality of the documents delivered as part of the project.
CDG.02	**M**	The Contractor shall maintain records of all project documents, including at least the following details: • Title • Purpose and brief description • Version / history • Status • Date • Format, file details (e.g. hash code for verification)
CDG.03	**M**	The Contractor shall ensure the delivery and development, coordination, and up-to-date maintenance of all documents required for project management processes (see the relevant section).
CDG.04	**M**	The Contractor shall develop and deliver at least the following documents related to the SRV: • Technical Design Document (TDD) for the information system (as detailed later in this table); • Database architecture document including an ERD (Entity-Relationship Diagram) and a CRUD matrix for data categories/information objects. • The RSV data model, including recognized reference standards. When presenting the data model, the methodology used for its development shall also be provided. • Document describing the digitised processes, including: BPMN diagrams, state diagrams, RACI matrix, etc. • Documentation of the APIs used for integration with other components. • SDK (Software Development Kit) for custom-developed components and other application components delivered as open source.
CDG.05	**M**	The Contractor shall develop and deliver all documentation required for the deployment, installation, administration, configuration and maintenance of the SRV and its supporting components. These shall include at least the following: • Detailed installation and deployment guide and instructions (including at least: installation of SRV components, hardware and software requirements, platform description and configuration, application configuration, and disaster recovery procedures).

Identifier	Mandatory status	Description of requirement
		• Operations manual intended for developers, aimed at providing a high-level understanding of the system's structure and organisation, enabling its maintenance and further development as needed; • Troubleshooting guide, which shall include a description of all error codes and exceptions and how to handle them; • Administrator's Guide (shall include the description of all ; • Guide for other specific roles (as per the functional requirements); • User Guide; • Guide to configuring and maintaining all system components in operation; • Guides for performing system data backups and restoration; • Instructions/guide for external users; • Training materials (used within the UAT process).
CDG.06	**M**	All documents prepared and delivered by the Contractor shall be in Romanian.
CDG.07	**M**	The Contractor shall be responsible for the quality and completeness of the delivered documents, ensuring that they are complete, detailed, accurate and sufficient for the activities and purposes for which they are intended.
CDG.08	**M**	The documents requested and delivered as part of the project shall also be subject to maintenance and support during the periods following the completion of implementation. Accordingly, the Contractor shall ensure that they are kept up to date and that any shortcomings, omissions or inconsistencies identified after their acceptance or following the completion of implementation are remedied.

The Technical Architecture Document (CDG.04) shall include at least the following (with a sufficient level of detail):

- The use case model and the functional requirements, including the relationships between them.
- The system components, including a narrative description of all components, the relationships between them, and the integration interfaces with other systems or external components.
- Roles and access profiles, and their interactions within the system and with external entities.
- The deployment model, including a narrative description of all nodes and the relationships between them. It shall also include the exact specifications of the equipment and operating environments required for the system to operate under normal conditions, as well as the specifications for a minimum acceptable/required configuration.

User Guide (CDG.05)

The Contractor shall provide a guide containing instructions and guidance for CEC users, as well as for other users, on how to use the SRV. The User Guide shall be distributed electronically in PDF and editable formats. The User Guide shall be written for users with an intermediate level of IT skills and shall include a detailed explanation of how to use the System, the responsibilities of each user role, the System's functionalities, and other relevant information.

The User Guide shall have a dual purpose: to serve as a desk reference or library resource, and as training material for any training courses conducted. In the case of a training course, the User Manual shall be printed and distributed to training participants.

Administrator's Guide (CDG.05)

The Administrator's Guide shall describe the full set of components and control measures used for configuration and shall also include guidance on managing users and their roles.

Project reporting requirements

The Contractor shall ensure regular and structured reporting to CEC throughout the entire project (implementation, go-live and the maintenance period), to ensure transparency, control and timely decision-making. Reporting shall be carried out using a standard template agreed at the start of the project and through common channels: the project repository and the ticketing system.

Monthly progress reports

The Contractor shall deliver monthly progress reports throughout the implementation phase. The requirements regarding the monthly reports are set out in Table 13.9:

Table 13.9. Requirements for monthly progress reports

Identifier	Mandatory status	Description of requirement
CRP.01	**M**	The monthly report shall include the overall project status (green/yellow/red), progress against the plan and key achievements, as well as the objectives for the following month
CRP.02	**M**	The report shall identify new risks and the status of existing ones, critical issues and the measures applied, as well as points requiring decision or involvement from CEC
CRP.03	**M**	Monthly reports shall be delivered by the 5th day of each month for the previous month, in PDF format
CRP.04	**M**	The Contractor shall present the monthly report at a status meeting with CEC (duration: 1–2 hours)

14. Warranty, maintenance and post-implementation support

Scope and coverage

The Contractor shall describe in detail the activities to be carried out to meet the stated requirements, providing sufficiently detailed information on how it intends to deliver the requested services to the required standard, as well as information on its technical, organisational and competency capabilities, demonstrating its ability to deliver at the required level.

The general requirements regarding warranty, maintenance and post-implementation support are set out below (see also the delineation of maintenance services presented below).

Table 14.1. General requirements for warranty, maintenance and post-implementation support

Identifier	Mandatory status	Description of requirement
CGG.01	**M**	The Contractor shall provide maintenance and support services for the SRV for a period of at least one year from the date of final acceptance and commissioning, to ensure stable and secure system operation, remedy defects, apply security updates, and provide operational assistance to CEC, including during electoral periods.
CGG.02	**M**	The price of the initial development and implementation contract shall include all post-implementation support and maintenance services, except for development services.
CGG.03	**M**	The price of the initial development and implementation contract shall also include, at the Beneficiary's request, the provision by the Contractor of 100 person-days of development services, as defined in these Terms of Reference.
CGG.04	**M**	All operational errors identified during the warranty period shall be remedied at the Contractor's expense (these activities shall not be considered development activities and shall not be counted towards the 100 person-days allocated to development during the warranty, support and maintenance period).
CGG.05	**M**	After one year of warranty, maintenance and post-implementation support services, CEC may request an extension of the services. The Contractor shall be obliged to accept the subsequent provision of services for a period of at least five years, under the conditions set out in these Terms of Reference and in the Contractor's offer (*e.g. service levels, pricing, etc.*).
CGG.06	**M**	The Contractor shall provide support in resolving incidents related to the SRV, regardless of the cause of the incident (e.g. application errors, system software issues, issues in external applications, human error, etc.).
CGG.07	**M**	Support services shall be provided under a Service Level Agreement (SLA), which shall be annexed to the Agreement signed between the Parties. The Agreement shall set the levels of post-implementation support and maintenance services, based on the requirements set out in these Terms of Reference.
CGG.08	**M**	Support services shall be delivered remotely. Where necessary, the Contractor's specialists shall travel to the premises of CEC.
CGG.09	**M**	The Contractor shall submit monthly reports to the CEC on the services provided and the service levels. The reports shall also include information on actions undertaken or planned by the Contractor to improve service quality.
CGG.10	**M**	Post-implementation support and maintenance services shall be based on best practices in project management and IT service management (*e.g. ISO 20000, ITIL, etc.*).
CGG.11	**M**	For each request received, the Contractor, together with CEC, shall explicitly classify the type of intervention: Incident/Defect (covered under

Identifier	Mandatory status	Description of requirement
		maintenance) or Change Request / Service Request (with effort estimated separately), along with a clear justification for the classification.

Delineation: maintenance (included) vs new developments

Maintenance services shall include:

- Technical support for users and administrators in accordance with the agreed model
- Incident management and issue resolution
- Remediation of vulnerabilities and application of security patches to components delivered or configured by the Contractor
- Support for operations and monitoring
- Operational consultancy during critical periods (elections)
- Updating technical documentation when interventions result in operational or configuration changes

The Contractor shall clearly distinguish between activities included in the Maintenance Agreement and additional developments billed separately:

Corrective maintenance (included in the Agreement) – rectification of defects or errors that prevent or degrade the system's operation in accordance with the approved functional and non-functional requirements. This includes logic errors, runtime errors (crashes), performance issues, integration errors with external systems and services (SRP, SAISE, etc.), reporting issues, incorrect validations, incorrect permissions, and workflows that do not operate in accordance with the specifications.

Adaptive and preventive maintenance (included within reasonable limits) – adjustments necessary to ensure secure operation and compatibility with the technological environment, including: application of security patches for identified vulnerabilities, minor version updates of libraries or frameworks (where current versions reach end-of-life), configuration adjustments for performance optimisation, and adaptations to minor changes in external systems' APIs (provided these do not fundamentally alter the integration logic).

New developments / functional changes (not included; billed separately) – functional extensions requested by the CEC that were not part of the initial requirements, new complex reports requiring new business logic, workflow changes requested by the CEC, integration of new systems not foreseen in the ToR requiring adjustments to components or services, changes required by major legislative amendments (e.g. to the Electoral Code) necessitating substantial rewrites of the logic (not merely parameter adjustments), and migration to entirely different technological platforms. These are handled through Change Requests, with effort estimation, formal approval and separate planning.

Development services during the warranty and support period

Table 14.2. Requirements for the change and development management process

Identifier	Mandatory status	Description of requirement
CMD.01	**M**	A request from the CEC shall be considered a change or development only if the functionality requested is not already provided by the SRV, or is provided in a manner different from that requested (requests relating to the correction of functionalities and defects are excluded).
CMD.02	**M**	The implementation of changes and developments shall be carried out in accordance with the requirements set out in the "Change Management" subchapter below.
CMD.03	**M**	Development services shall include: • modification of the existing functionalities; • implementation of new functionalities • implementation of new integrations and data flows.
CMD.04	**M**	The Contractor shall provide standard forms, including a description of the completion requirements, for all types of changes and developments.

Identifier	Mandatory status	Description of requirement
		If necessary, the Contractor shall provide support and guidance in completing the relevant forms.
CMD.05	**M**	Development and change implementation services, additional to those included in the Agreement (100 person-days), may be requested by the CEC and provided by the Contractor on the basis of additional agreements signed between the Parties.
CMD.06	**M**	The Contractor shall provide a detailed estimate for each request for change or development. This shall include at least: - the number of person-hours for each type of resource involved (e.g. developer, PM, architect, QA). - The implementation timeframe. - The implementation plan.

Communication channels and tools

The Contractor shall ensure a formal mechanism for the recording and tracking of requests (of any type, in accordance with the agreed categorisation):

Ticketing system: a ticketing tool (e.g. Jira Service Management, Redmine, ServiceNow, or another tool agreed with the CEC) shall be used to manage all requests. The request management workflow, as well as the roles and persons with access, shall be agreed through the signing of an SLA.

Communication channels:

- Email: a dedicated support email address (e.g. support-rsa@furnizor.org) for standard requests.
- Phone/Hotline: a dedicated number for critical P1/P2 incidents, available during working hours (8×5 or in accordance with the SLA).
- Secure chat (optional): a channel for rapid communication with the CEC team.

Points of contact: The Contractor shall designate and communicate to the CEC the list of contact roles. Support Engineer (first line), Senior Engineer (technical escalation), Team Lead or Manager (managerial escalation), Account Manager (contractual relationship).

Record-keeping: All tickets, support emails, intervention logs and resolution documents shall be retained for at least the duration of the maintenance contract plus one year, for audit and traceability purposes.

Service levels

The parameters defining the level of support services are as follows:

- Response Time (RT) – the time within which the Contractor shall respond to a support request, diagnose the situation and determine the actions required to resolve it.
- Resolution Time (RST) – the target time within which the Contractor is expected to complete the actions within its area of responsibility in order to fully resolve the request.

Requests for support and post-implementation maintenance services shall be classified based on their importance for the CEC. The importance for the CEC shall be assessed based on the impact (actual or potential) of the event that triggered the request on the quality parameters of the SRV's operation (including all components delivered or configured by the Contractor).

The criteria for classifying the importance of requests are set out below. In determining importance, one or more quality parameters shall be considered, with the parameter having the highest value (e.g. availability) taken as the reference.

Table 14.3. Priority classification of service, maintenance and support requests (including incidents).

Classification	Impact on the quality parameters for the operation of the applications
Critical (P1)	*Availability:* The SRV is unavailable to all or the majority of users. Important operations need to be carried out as soon as possible (within hours).

Classification	Impact on the quality parameters for the operation of the applications
	Usability: key business functions are unavailable for use. There are no alternative procedures or functionalities. *Performance:* response times to user queries render the information system effectively unavailable *Security:* there are major risks of compromise to the confidentiality, integrity or availability of data.
High (P2)	*Availability:* The SRV is unavailable to a large proportion of users. Important operations and activities due by the start of the next day are affected. *Usability:* key business functions are available with limitations. *Performance:* response times to user queries significantly affect the execution of key processes. *Security:* there are high risks of compromise to the confidentiality, integrity or availability of data.
Normal (P3)	*Availability:* The SRV is unavailable to some users. Operations and activities that must be carried out within the next three working days are affected. *Usability:* the system's business functionality is partially available. *Performance:* response times to user queries moderately impact the execution of business processes. Security: there are risks of compromise to the confidentiality, integrity or availability of data.
Low (P4)	*Availability:* The SRV is unavailable to a limited number of users. No operations or activities to be carried out within the next three working days are affected. *Usability:* the system's business functionality is insignificantly affected. Alternative procedures and functionalities exist. *Performance:* response times to user queries are higher than usual. Business processes are not affected. *Security:* there are minor risks of compromise to the confidentiality, integrity or availability of data.

When submitting a request for post-implementation support and maintenance services, CEC shall assign the priority classification to the request. CEC shall provide concise and explicit information to explain the classification. CEC may reclassify requests submitted, based on changes in the context of those requests. The Contractor shall apply the following priority classification (applicable to both the implementation and maintenance periods):

Table 14.4. Resolution time for service, maintenance and support requests (including incidents)

Priority	Response Time (RT)	Resolution Time (RST)
Critical (P1)	5 min	60 min
High (P2)	60 min	End of day
Normal (P3)	24 h	3 days
Low (P4)	3 days	Best effort*

Table 14.5. Requirements for managing maintenance and support services

Identifier	Mandatory status	Description of requirement
CMS.01	**M**	The Contractor shall provide support services on working days, in accordance with the legislation of the Republic of Moldova, between 08:00 and 18:00 (local time in the Republic of Moldova).
CMS.02	**M**	The Contractor shall adjust the priority of the request in consultation with the CEC.

Identifier	Mandatory status	Description of requirement
		If the Contractor modifies the priority, they shall provide appropriate justification.
CMS.03	**M**	For any activity involving a change in priority, CEC shall receive a notification both via the agreed service request management platform and by email.
CMS.04	**M**	For P1 and P2 requests, the Contractor shall designate a contact person responsible for periodically informing CEC of developments and changes.

Special support arrangements during electoral periods

Given the critical importance of the SRV to the electoral process, the Contractor shall ensure enhanced support arrangements during periods designated by CEC as critical (typically: 7 days before election day, election day, and 3 days thereafter). CEC shall inform the Contractor at least one month in advance of such periods.

Table 14.6. Requirements for the management of maintenance and support services under special arrangements

Identifier	Mandatory status	Description of requirement
CRS.01	**M**	The Contractor shall ensure the designation of a single point of contact (Support Lead) responsible for rapid coordination with CEC, available 24/7 via phone and email during the critical period.
CRS.02	**M**	The Contractor shall be informed by CEC of the electoral period during which special support arrangements may be required. Special support arrangements shall be initiated based on an official request from CEC, submitted via the ticketing system or by email.
CRS.03	**M**	The Parties shall coordinate and agree on the critical time windows during which special support arrangements are required. By default, during electoral periods, the following time window shall be considered as subject to special support arrangements: 7 days before election day, election day, and 3 days thereafter; however, the duration of the period and the support arrangements shall be agreed on a case-by-case basis for each election.
CRS.04	**M**	During periods under special support arrangements, the Response Time (TR) and the Resolution Time (TS) for P1 and P2 service, maintenance and support requests (including incidents) shall be halved.
CRS.05	**M**	The Contractor shall participate in daily briefings with the CEC team during the critical period (15–30 minutes, online or on-site) to ensure alignment on the operational context and to prevent issues.
CRS.06	**D**	At CEC's request, the Contractor shall ensure the physical presence of a specialist at the CEC premises, as required. Note: these activities shall be accounted for and paid separately, or charged against the service days included in the Agreement (CGG.03).
CRS.07	**M**	At CEC's request, or in duly justified emergency situations, the Contractor shall ensure the participation of the Support Lead (CRS.01) in daily briefings with the CEC team (15–30 minutes, online or on-site).

Change management

All changes applied to the SRV in the context of post-implementation support and maintenance services shall be managed in accordance with a mature change management process. The table below sets out the requirements for the organisation of change management. These requirements shall be incorporated into the Maintenance and Support Agreement (Annex to the main contract).

Table 14.7. Requirements for change management

Identifier	Mandatory status	Description of requirement
CMM.01	**M**	In its tender, the Contractor shall include information on the proposed approach to change management, the methodology to be applied, etc.
CMM.02	**M**	The Contractor shall provide a description (e.g. a procedure) of the change management process, setting out all practical aspects of the process, including stages, control measures, tools used, etc.
CMM.03	**M**	The aforementioned procedure (CMM.02) shall be coordinated with CEC prior to the initiation of implementation activities. The coordinated and agreed version shall be used throughout the project, including during the maintenance and support phase.
CMM.04	**M**	All changes made to SRV components shall be implemented in accordance with a mutually agreed change management process. Changes that may have a significant impact on the SRV's quality parameters shall be authorised by CEC prior to their implementation in the production environment. Mandatory elements for this type of change shall be: • testing in the test environment; • the change implementation plan; • the rollback plan; • post-implementation review and testing. The Contractor shall maintain a record of all changes in a Change Register. CEC shall have read-only access to the Register.

Reporting and performance indicators

Table 14.8. Requirements for reporting during the maintenance and support period

Identifier	Mandatory status	Description of requirement
CMR.01	**M**	The Contractor shall provide monthly support reports, to be delivered within the first 5 days of the month following the reference month. Each monthly report shall contain the information set out in Table 14.9.
CMR.02	**M**	In addition to the monthly reports, the Contractor shall deliver quarterly reports summarising the situation over a three-month period, including: medium-term trend analysis, an overall assessment of system stability, strategic recommendations for improvement, and comparative statistics with the previous quarter.
CMR.03	**M**	After each electoral period, a dedicated post-election report shall be delivered, focusing on incidents and issues arising during the critical period, actual resolution times, lessons learned, and recommendations for future elections.
CMR.04	**M**	Reports shall be delivered in PDF format together with Excel files containing raw data for detailed analysis. On a quarterly basis, the reports shall be presented in a review meeting with CEC representatives for discussion and to ensure alignment of expectations.
CMR.05	**M**	The Contractor shall ensure an efficient and transparent process for monitoring performance indicators for all requests. The Contractor shall ensure compliance with the requirements set out in Table 14.10.
CMR.06	**M**	The Contractor shall ensure reporting to CEC and escalation of cases to CEC management where requests are delayed in resolution due to insufficient involvement of CEC representatives or technical issues on the CEC side.

Table 14.9. Requirements for the structure and content of the monthly reports

Report section	Content
Executive summary	Total number of requests, resolution rates, SLA compliance per indicator, comparative analysis with the previous period, key information, and conclusions.
Analysis of requests	Detailed information on requests (tickets, etc.), broken down by priority, resolution times, and by other relevant criteria, including: P1/P2/P3/P4 — received, resolved, in progress, cancelled, etc.
SLA performance	Percentage compliance with response and resolution times by priority level Tickets that breached SLA, with explanations for each case
Top issues	Top 5 causes of incidents (e.g., unstable SRP integration, search performance issues) Identified trends: recurring issues, gradual degradation
Preventive measures	Actions taken or planned to prevent the recurrence of issues Recommendations for CEC on operational improvements
Applied changes	List of patches, hotfixes and updates installed during the reporting month Impact of each change: improvements made and issues resolved
Planning for the next month	Scheduled maintenance, planned updates and actions to be implemented.

Table 14.10. Monitored key performance indicators

Indicator	Description	Target
SLA Compliance Rate	Percentage of tickets resolved within agreed timeframes	≥95% for P1/P2 ≥90% for P3
MTTA (Mean Time to Acknowledge)	Average time from reporting to first response	In accordance with the SLA, by priority level
MTTR (Mean Time to Resolve)	Average time from reporting to final closure	In accordance with the SLA, by priority level
First Contact Resolution Rate	Percentage of tickets resolved at first point of contact (without escalation)	Tracked for continuous improvement
Reopen Rate	Percentage of tickets reopened after being closed	<5%

15. Qualification requirements for Tenderers and the proposed implementation team and timeline

The Contractor shall include in the technical proposal summary information on the following key personnel to be involved in the project activities and their qualifications (CVs of the key personnel must be included in the proposal):

Table 15.1. Requirements for the IS "SRV" implementation team

No.	Role	Experience and qualifications
1.	**Project Manager:** Leads the project team on behalf of the Contractor and is primarily responsible for fulfilling the Contractor's obligations under the Project. Ensures the availability of the necessary experts of the Contractor in accordance with the Project Activity Plan, organises and coordinates the project activities assigned to the Contractor's team, and ensures that they are carried out in line with the requirements and agreed timeframes. Develops and maintains the project management plan, the risk register, the project communications plan, and the project plan. Ensures effective communication, and coordinates and facilitates interaction and collaboration between the Contractor's project team and the Beneficiary's project team, as well as with external partners.	• University degree in Management, Engineering, ICT or another relevant field • At least 5 (five) years of experience in project management of projects on developing IT applications/systems, services, etc. • Experience in at least 2 (two) similar complexity software development projects • Relevant experience in business process analysis • Proven certification in Project Management (PMP, PRINCE2, CSM, CBAP / CCBA, ISTQB, AZURE, TOGAF, SAFe, etc.) would be an asset • Proficiency in Romanian and English languages
2.	**Business Analyst with Training responsibilities:** Responsible for analysing business needs and translating functional requirements into clear, feasible, and actionable technical specifications for the development team. The expert collaborates closely with the Beneficiary and other stakeholders to identify, document, refine, and prioritise functional and non-functional requirements based on project value and implementation needs. The role also includes ensuring a common understanding of requirements among all parties involved in the project and supporting their correct interpretation and application throughout the development process. In addition, the expert participates in the testing, verification, and validation of developed functionalities to ensure compliance with agreed requirements and user expectations, while also organising and/or delivering training activities and preparing related training materials and user guidance documentation.	• University degree in Management, Engineering, ICT or another relevant field • At least 5 (five) years of experience in business analysis • Experience as Business Analyst or similar position in at least 2 (two) software development projects of similar complexity • Relevant certification such as CBAP, General Business Analysis Certifications, Product Ownership or BPM would be an asset • Proven experience in delivering user training for information systems in at least 2 (two) projects implemented within the past 3 (three) years • Proven experience in preparing documentation and training materials for end users, including for the UAT process • Proficiency in Romanian and Russian languages
3.	**System Architect:** The System Architect is responsible for designing and defining the system architecture, ensuring that it is coherent, efficient and scalable, in line with the SRV requirements and objectives. The System Architect works with the development team to	• University degree in Computer Science or another relevant domain • At least 5 (five) years of professional experience as a System Architect in the design, development and implementation of information systems

No.	Role	Experience and qualifications
	design and define the system's structure and components, as well as its integration with other internal and external components. The System Architect oversees the implementation of the defined architecture and ensures that software components are correctly integrated and that the system operates as specified.	• Experience as a System Architect in at least 2 (two) projects of similar complexity implemented within the last 3 (three) years • Experience in unit testing, continuous integration and DevOps practices • Certifications in information systems architecture or design (e.g. TOGAF 9, CTA or equivalent) is an asset • Proficiency in Romanian and English or Russian languages
4.	**Team Leader acting as Senior Software Developer and responsible for UX/UI compliance:** Responsible for leading and coordinating the software component development process, including coding, integration, and testing activities. As a Team Leader - supervises and coordinates the work of other technical experts involved in development and ensures effective communication and collaboration within the development team. The role also includes overseeing the documentation of UX/UI requirements, ensuring their proper translation into technical specifications, and contributing to the assessment of whether the implemented UX/UI solutions comply with the agreed requirements and user expectations.	• University degree in Computer Science or another relevant domain • At least 5 (five) years of experience in developing information using the proposed technology stack • Participated in at least 2 (two) similar complexity projects in the last 3 (three) years • Experience in unit / module testing, continuous integration and DevOps practices • Experience in information systems integration and in designing and implementing data exchange interfaces (APIs) using SOAP and REST • Proven experience in design tools such as Figma (advanced level), FigJam, etc.; experience in UX principles, wireframing, prototyping and accessibility (WCAG); or experience in collaborating within design systems and maintaining design documentation • Certifications in any technology from the proposed technology stack mentioned above is an asset • Proficiency in Romanian and English languages
5.	**Software Developer with Database Administration responsibilities** Responsible for designing the overall data architecture and for the development, administration, and maintenance of the database environment. The expert shall define the data architecture and taxonomy of structured information objects, design the architecture of electronic registers, and develop the conceptual database model, including stored procedures. The role also includes configuring database access rights and privileges for different user categories, implementing database backup and recovery mechanisms, and developing data migration and initial data population procedures to ensure data integrity, security, and system reliability.	• University degree in Computer Science or another relevant domain • At least 5 (five) years of experience in software development as a Database Developer/Administrator, using the proposed technology stack • Experience in a similar position in at least 2 (two) similar complexity projects in the last 3 (three) years • Experience in unit testing and continuous integration • Certification in database technologies and in the proposed technology stack is an asset

No.	Role	Experience and qualifications
	The role includes the definition of the strategy and procedures for data migration from existing systems, integration with data sources, development and configuration of ETL mechanisms, and preparation and load of the datasets required for system operation.	
6.	**Software Developer with DevOps responsibilities:** Responsible for integrating and coordinating individual software components into a cohesive, stable, and functional solution. The expert shall ensure the interoperability and proper interaction of software modules and systems developed by different team members, support deployment and integration processes, and contribute to maintaining a reliable development and operational environment. The role includes coordinating component integration activities, troubleshooting integration issues, and ensuring that the overall solution functions in accordance with the defined technical requirements and architecture.	• University degree in Computer Science or another relevant domain • At least 5 (five) years of experience in software development using the proposed technology stack • Experience in a similar position in at least 2 (two) similar complexity projects in the last 3 (three) years • Experience and competencies in continuous integration and continuous delivery for information systems of similar complexity • Experience in unit testing and DevOps practices • Certification in continuous integration and continuous delivery (CI/CD) for information systems in the proposed technology stack is an asset
7.	**QA Expert:** Key expert responsible for ensuring the quality of SRV development and implementation processes, including functional and non-functional testing, also using automated methods. Responsible for ensuring the quality of all aspects related to development and implementation, including documentation.	• University degree in Computer Science or another relevant domain • At least 5 (five) years of experience in testing information systems • Experience in a similar position in at least 2 (two) similar complexity projects in the last 3 (three) years • Proven experience in functional and non-functional testing of information systems, in accordance with the methodology proposed • Proven experience in performance testing (load and stress testing) and security testing, covering at least the OWASP Top 10 vulnerabilities • Proven experience in applying automated testing to information systems • Certification in software testing (e.g. ISTQB) and in using the proposed technology stack is an asset
8.	**Trainer:** Responsible for developing user, administrative and architectural documentation. Ensures the organisation and delivery of training for the user categories specified in these Terms of Reference and ensures the development of appropriate training materials. Ensures the organisation of the UAT process and other types of testing involving end users.	• Proven experience in organisation and delivery of training on information systems • Experience in developing user, administrative and architectural documentation • Experience in the organisation of the UAT process and other types of testing involving end users

The qualifications, experience and competences of the other team members (non-key personnel) shall correspond to the tasks and duties under the project, in strict accordance with the proposed methodology and technologies. Each non-key expert must be included in the tender and must, at a minimum, have a command of Romanian and Russian at a level sufficient to perform the assigned functions and tasks.

16. Deliverables and implementation stages of the SRV

The indicative action plan and implementation deadlines are as follows:

Activity	Deliverable	Maximum indicative duration (weeks)	Predecessor activity
Activity 1: Kick off meeting with the CEC and the UNDP Project Team	**Deliverable 1:** Detailed minutes of the meeting confirming the scope, approach and work plan – developed, submitted and approved by the CEC and UNDP Project Team	1	-
Activity 2: Develop a detailed Project Implementation Plan	**Deliverable 2:** Project Implementation Plan confirming the roles of stakeholders, focal points, deliverables, timeline, etc. – submitted and approved by CEC and UNDP Project Team	2	1
Activity 3: Develop a detailed System Architecture Document of the computer subsystem 'State Registry of Voters' of State Automated Information System 'Elections'	**Deliverable 3:** System Architecture Document, confirming the architecture and components, data architecture, technology stack, integrations and interfaces, non-functional requirements, deployment setup, operational considerations, etc. - submitted and approved by CEC and UNDP Project Team	6	2
Activity 4: Develop the computer subsystem 'State Registry of Voters' of State Automated Information System 'Elections'	**Deliverable 4:** Computer subsystem 'State Registry of Voters' of State Automated Information System 'Elections' fully developed in accordance with the approved System Architecture Document and technical specifications (Deliverable 3), including fully developed front-end and back-end, configured databases, implemented business logic, integrated interfaces with external systems. The subsystem should be functionally complete and integrated at information system level, deployed in the testing environment and demonstrated to CEC and UNDP Project Team	24	3
Activity 5: Preparation of Test Plans for the computer subsystem 'State Registry of Voters' of State Automated Information System 'Elections'	**Deliverable 5:** Test plans for User Acceptance Testing, Load & Stress Testing and Automation Testing Plans, including the strategy, scope, approach, resources, schedule, etc. - completed and validated by the CEC and UNDP Project Team	1	-
Activity 6: Execute testing to verify functionality, performance, and compliance with requirements	**Deliverable 6:** Assisted testing conducted with all type of users and detailed report proving that the system has been tested and issues have been addressed - reported and validated by to the CEC and UNDP Project Team	4	5
Activity 7: Training the Users	**Deliverable 7:** 7.1. User manual, System installation and configuration manual, API integration guide and samples, Training materials – developed and presented to the CEC and UNDP Project Team 7.2. At least 2 user training sessions for CEC (the CEC will provide the necessary arrangements and logistics for organizing the training) – conducted and	2	6

	post training report submitted to the CEC and UNDP Project Team		
Activity 8: Implementation the computer subsystem 'State Registry of Voters' of State Automated Information System 'Elections'	**Deliverable 8:** 8.1. The system successfully configured and deployed in the Production Environment in compliance with all TOR requirements, with no critical or high-severity unresolved defects, evidenced by a Formal Acceptance Certificate validated by the CEC confirming successful commissioning. 8.2. Source Code and deployment documentation, System architecture and technical documentation, Security and testing documentation, User and administrator guides – presented and delivered to the CEC and the UNDP Project Team. 8.3. Signed SLA covering the 12-months maintenance, warranty, and technical support services - formally approved by the CEC and UNDP Project Team	2	-
Activity 9: Maintenance, Warranty and Technical Support Services for 12-months following the commissioning of the system	**Deliverable 9:** Report on Maintenance, Warranty and Technical Support Services for 12-months period following the system commissioning – formally approved by the CEC and the UNDP Project Team	52	8

Overall, the time needed to design, develop the system, and conduct testing and remove errors/non-conformities is estimated at maximum indicative duration of 42 weeks.

Note: Certain implementation activities can be performed concurrently.

Annex 1. Data sets for the State Registry of Voters

1. Involved Institutions

ID	Abbreviation	Institution Name
1	ASP	Public Services Agency
2	ADJAJ	Agency for Digitalization in Justice and Judicial Administration
3	SFS	State Tax Service
4	MEC	Ministry of Education and Research
5	ANP	National Administration of Penitentiaries
6	MMPS	Ministry of Labor and Social Protection
7	AGCC	Agency for Geodesy, Cartography and Cadastre
8	CNDDCM	National Council for Determining Disability and Work Capacity
9	CTICE	Centre for Information and Communication Technologies in Education
10	MJ	Ministry of Justice

2. Source Information Systems

ID	Abbreviation	System Name	Owner / Operator
1	RSP	State Register of Population	ASP
2	RSUD	State Register of Legal Entities	ASP
3	PIGD	Integrated Case Management Program	ADJAJ
4	SI DDCM	Information System "Determination of disability and work capacity"	CNDDCM
5	SIGS Geodata	State Geographical Information System "Thematic geoportal for spatial data of the Agency for Geodesy, Cartography and Cadastre 'GEODATA.GOV.MD'"	AGCC

3. General Data Sets

ID	Data Set / Field Name	Description	Institution	Method of Acquisition	System
1	Court decision	Court decision on deprivation of voting rights, citizenship, or determination of incapacity (e.g., requires guardianship)	ADJAJ	PDF format, with semi-automated processing	PIGD
2	Geospatial data	Spatial data required for forming various map layers and representations on existing maps (WMS, WFS)	AGCC	To be determined feasibility	SIGS Geodata
3	Diplomatic missions abroad	Data on the diplomatic missions of the Republic of Moldova	MAE	Obtained in digital format, documents (PDF, DOCX, XLSX)	Currently no systems can provide data
4	Polling stations abroad	Data on the locations where polling stations are located/set up	MAE	Obtained in digital format, documents (PDF, DOCX, XLSX)	Currently no systems can provide data

4. Detailed Structure of Data Flows

4.1. Data Set: Person

ID	Field	Description	Required	Format	Institution	System	Integration
1.1.	IDNP	Unique personal identification number (IDNP). May be missing in case of persons who renounced the IDNP	Yes	String (13)	ASP	RSP	Mconnect
1.2.	Nume (lastname)	Last name, Person's family name. A name typically shared by members of a family.	Yes	String (30)	ASP	RSP	Mconnect
1.3.	Prenume (firstname)	First name, Person's given name. A given name or multiple given names that identify a person within a family.	Yes	String (30)	ASP	RSP	Mconnect

ID	Field	Description	Required	Format	Institution	System	Integration
1.4.	Sex (sexcode)	Sex (sexcode), Gender code (contains values from the person's sex classifier - CF 37603221.0037.01)	Yes	SexCode	ASP	RSP	Mconnect
1.5.	Data Nașterii (birthdate)	Date of Birth (birthdate), Person's date of birth. Format dd-mm-yyyy (dd - day of the month as a number from 01 to 31, mm - month as a number from 01 to 12, yyyy - year as a four-digit number)	Yes	Date	ASP	RSP	Mconnect
1.6.	Decedat (dead)	Deceased (dead), Indication of the natural person's death. Takes the value: - true, if the person is deceased; - false, if the person is alive	Yes	Boolean	ASP	RSP	Mconnect
1.7.	Data decesului (deathdate)	Date of death (deathdate), Date of death. Format dd-mm-yyyy (dd - day of the month as a number from 01 to 31, mm - month as a number from 01 to 12, yyyy - year as a four-digit number)	Yes	Date	ASP	RSP	Mconnect
1a	Cetățean RM (citizenRm)	RM Citizen (citizenRm), Indicates if the person is a citizen of the Republic of Moldova	Yes	Boolean	ASP	RSP	Mconnect
1b	Valabilitate doc. (validity)	Document Validity (validity), Indicates if the identity document is valid	Yes	Boolean	ASP	RSP	Mconnect
1.8.	Țară Naștere	Country of Birth (birthcountrycode), Code of the country of birth.	Yes	CountryCode	ASP	RSP	Mconnect

ID	Field	Description	Required	Format	Institution	System	Integration
	(birthcountrycode)	Contains values from the localities classifier CF 37603221.0026.01 "Localities"					
1.9.	Regiune Naștere (birthregion)	Region of Birth (birthregion), District of birth of the person	Yes	string(60)	ASP	RSP	Mconnect
1.10.	Localitate (birthlocality)	Locality of Birth (birthlocality), Locality of birth of the person	Yes	string(60)	ASP	RSP	Mconnect
1.11.	Cetățenie (citizencode)	Citizenship (citizencode), Legal status of the person. Contains values from the classifier CF 37603221.0066.03 "Citizenship". Citizenship rights include rights such as the right to vote, to receive certain protection from the community, or the issuance of a passport	Yes	CitizenCode	ASP	RSP	Mconnect
1.12.	Document (identdocument)	Document (identdocument), The identity document of the person	Yes	identdocument	ASP	RSP	Mconnect
1.13.	Adresă	Address, Data regarding the domicile or temporary residence of the natural person. Contains the domicile address data from the residence visa data. In case the natural person has a permanent and temporary residence visa, the address will be filled in with the temporary residence visa data	Yes	address	ASP	RSP	Mconnect

ID	Field	Description	Required	Format	Institution	System	Integration
1.14.	Registration	Registration, List of home address and/or temporary residence registrations	Yes	Stirng	ASP	RSP	Mconnect
1.15.	Poza (GraphicData)	Photo (GraphicData), Graphical data of the natural person. Latest photo from RSP	Yes	GraphicData	ASP	RSP	Mconnect
1c	Status conflict (statusConflictCode)	Status conflict (statusConflictCode), Status conflict code upon import	Yes	Integer	ASP	RSP	Mconnect
1d	Accept conflict (acceptConflictCode)	Accept conflict (acceptConflictCode), Conflict acceptance code	Yes	Integer	ASP	RSP	Mconnect
1e	Reject conflict (rejectConflictCode)	Reject conflict (rejectConflictCode), Conflict rejection code	Yes	Integer	ASP	RSP	Mconnect

4.2. Data Set: Document

ID	Field	Description	Required	Format	Institution	System	Integration
1.12.1.	Tip document (doctypecode)	Document type (doctypecode), Type of document. Contains values from the classifier CF 37603221.0265.03 "Document Type"	Yes	DocumentType	ASP	RSP	Mconnect
1.12.2.	Serie	Series, Document series	Yes	string(8)	ASP	RSP	Mconnect
1.12.3.	Număr	Number, Document number	Yes	string(20)	ASP	RSP	Mconnect
1.12.4.	Data Eliberării	Issue Date, Document issue date	Yes	Date	ASP	RSP	Mconnect

ID	Field	Description	Required	Format	Institution	System	Integration
1.12.5.	Data Expirării	Expiry Date, Document expiry date	Yes	Date	ASP	RSP	Mconnect
1.12.6.	Eliberat de (issuedby)	Issued by (issuedby), The issuing authority of the document	Yes	string(60)	ASP	RSP	Mconnect
1.12.7.	Statut (statuscode)	Status (statuscode), Document status. Contains values from the classifier CF 37603221.0300.02 "Status or reason for updating document status"	Yes	number	ASP	RSP	Mconnect

4.3. Data Set: Address

ID	Field	Description	Required	Format	Institution	System	Integration
1.13.1.	Țară	Country, Name of the state	Yes	String	ASP	RSP	Mconnect
1.13.2.	Regiune	Region, Name of the second-level administrative-territorial unit (district, municipality, UTA), or, as applicable, the name of the Gagauzia autonomous territorial unit	Yes	string(64)	ASP	RSP	Mconnect
1.13.3.	City	City, Name of the first-level administrative-territorial unit (municipiu, city, commune, village)	Yes	string(64)	ASP		
1.13.4.	Localitate	Locality, Name of the locality	Yes	string(64)	ASP	RSP	Mconnect

ID	Field	Description	Required	Format	Institution	System	Integration
1.13.5.	Cod CUATM (AdministrativeCode)	CUATM Code (AdministrativeCode), Locality code (according to the classifier of administrative-territorial units - CUATM)	Yes	String	ASP	RSP	Mconnect
1.13a	Stradă cod (streetcode)	Street code (streetcode), Street code according to RSP	Yes	Integer	ASP	RSP	Mconnect
1.13.6.	Stradă	Street, Name of the traffic artery or public traffic area to which the addressable object has an exit	Yes	string(64)	ASP	RSP	Mconnect
1.13b	Sufix casă (houseSuffix)	House suffix (houseSuffix), Suffix of the building number (e.g., A, B)	No	String	ASP	RSP	Mconnect
1.13.7.	Casă (Building)	House (Building), Building number	Yes	string(8)	ASP	RSP	Mconnect
1.13.8.	Bloc	Block, Block number. The block number is an integral part of the building number. The block number is written after the "/" sign.	Yes	string(8)	ASP	RSP	Mconnect
1.13.9.	nr.apartament	Apartment no., Number of the isolated room	Yes	string(8)	ASP	RSP	Mconnect
1.13c	Sufix apartament (apSuffix)	Apartment suffix (apSuffix), Suffix of the apartment number	No	String	ASP	RSP	Mconnect

4.4. Data Set: Registration

ID	Field	Description	Required	Format	Institution	System	Integration
1.14.1.	Tipul	Type, Code of the registration type (contains values from the home registration type classifier - CF 37603221.0264.01)	Yes	number	ASP	RSP	Mconnect
1.14.2.	Data înregistrării	Registration Date, Date of registration	Yes	DateTime	ASP	RSP	Mconnect
1.14.3.	Data Expirării	Expiry Date, Expiry date of the registration at the temporary residence	Yes	DateTime	ASP	RSP	Mconnect
1.14a	În conflict (isInConflict)	In conflict (isInConflict), Indicates whether the home registration conflicts with CEC data	Yes	Boolean	ASP	RSP	Mconnect

4.5. Data Set: Disability

ID	Field	Description	Required	Format	Institution	System	Integration
2.1	IDNP	IDNP, Unique personal identification number (IDNP)	Yes	String	MMPS (CNDDCM)		Mconnect
2.2	Grad dizabilitate	Disability degree, Established degree of disability	Yes	String	MMPS (CNDDCM)		Mconnect
2.3	Ultimul grad stabilit	Latest degree established, Latest category / latest degree recorded	Yes	String	MMPS (CNDDCM)		Mconnect
2.4	DisabilityStatus	DisabilityStatus, Status (Assigned a disability degree Yes/No)	Yes	boolean	MMPS (CNDDCM)		Mconnect

ID	Field	Description	Required	Format	Institution	System	Integration
2.5	DecisionNumber	DecisionNumber, Number of the decision (report)	Yes	String	MMPS (CNDDCM)		Mconnect
2.6	DecisionDate	DecisionDate, Date of the granting decision	Yes	DateTime	MMPS (CNDDCM)		Mconnect
2.7	Timp Valabilitate	Validity Period, Duration for which the disability is granted		String	MMPS (CNDDCM)		Mconnect
2.8	PpcmPercent	PpcmPercent, Percentage of loss of work capacity due to disability causes, according to the classifier	Yes	number	MMPS (CNDDCM)		Mconnect
2.9	DisabilityCause	DisabilityCause, Cause of disability	Yes	String	MMPS (CNDDCM)		Mconnect
2.10	From	From, Establishment of the disability degree (period from establishment or withdrawal of the disability degree)		DateTime	MMPS (CNDDCM)		Mconnect
2.11	Stabilit pe viață	Life-long establishment, indicates whether the degree is established for life	No	Boolean	MMPS (CNDDCM)		Mconnect

4.6. Data Set: Detention

ID	Field	Description	Required	Format	Institution	System	Integration
3.1	IDNP	IDNP, Unique personal	Yes	String	MMPS (CNDDCM)		Mconnect

ID	Field	Description	Required	Format	Institution	System	Integration
		identification number (IDNP)					
3.2	Stare de detenție	Detention status, Describes the state of detention in relation to the stages of serving the custodial sentence.	Yes	Integer	ANP		Mconnect
3.3	Statut de detenție	Detention status, Indicates if the person is in detention	Yes	Boolean	ANP		Mconnect
3.4	Loc detenție	Place of detention, Penitentiary / place where the person is located (Describes the place of detention during the period of serving the custodial sentence)	No	Boolean	ANP		Mconnect
3.5	PlaceOfDetention	PlaceOfDetention, Place of detention (code)	Yes	Integer	ANP		Mconnect
3.6	Regim	Regime, Type of detention regime	No	String	ANP		Mconnect
3.7	Perioada detenției	Detention period, End date of the detention period		Date interval	ANP		Mconnect
3.8	Număr dosar	Case number, File/case number, if it exists in the system	No	String	ANP		Mconnect
3.9	Acte de identitate valabile	Valid identity documents; Indicates whether		Boolean	ANP		Mconnect

ID	Field	Description	Required	Format	Institution	System	Integration
		the persindicatesvalid documents					

4.7. Data Set: Student

ID	Field	Description	Required	Format	Institution	System	Integration
4.1	IDNP	IDNP, Unique personal identification number (IDNP)	Yes	String	MEC (CTICE)	SIME	MConnect
4.2	IDNO Instituție învățământ	Educational institution IDNO, IDNO code, The institution where the student is enrolled	Yes	String	MEC (CTICE)	SIME	MConnect
4.3	Facultate	Faculty, Faculty where enrolled	No	String	MEC (CTICE)	SIME	MConnect
4.4	Statut student	Student status, The student's status in the system	Yes	String	MEC (CTICE)	SIME	MConnect
4.5	Localitate	Locality, Student's address, including the dormitory where accommodated	Yes	String	MEC (CTICE)	SIME	MConnect
4.6	City	City, Name of the first-level administrative-territorial unit (municipiu, city, commune, village)	Yes	String	MEC (CTICE)	SIME	MConnect
4.7	Localitate	Locality, Name of the locality	Yes	String	MEC (CTICE)	SIME	MConnect
4.8	Stradă	Street, Name of the traffic artery or public traffic area to which the addressable object has an exit	Yes	String	MEC (CTICE)	SIME	MConnect
4.9	Casă (Building)	House (Building), Building number	Yes	String	MEC (CTICE)	SIME	MConnect

ID	Field	Description	Required	Format	Institution	System	Integration
4.10	Sufix casă (houseSuffix)	House suffix (houseSuffix), Suffix of the building number (e.g., A, B)	No	String	MEC (CTICE)	SIME	MConnect
4.11	Bloc	Block, Block number. The block number is an integral part of the building number.	Yes	String	MEC (CTICE)	SIME	MConnect
4.12	nr.cameră	Room no., Number of the isolated room	No	String	MEC (CTICE)	SIME	MConnect

4.8. Data Set: Judicial Case

ID	Field	Description	Required	Format	Institution	System	Integration
5.1	CaseNumber	CaseNumber, The electronic number or unique identifier of the case		String	MJ (ADJAJ)	PIGD	MConnect
5.2	ID Dosar	Case ID, The identifier of the case		String	MJ (ADJAJ)	PIGD	MConnect
5.3	Number Dosar	Case Number, The case number		String	MJ (ADJAJ)	PIGD	MConnect
5.4	ParticipantRole	ParticipantRole, The type of the participant		String	MJ (ADJAJ)	PIGD	MConnect
5.5	CaseTitle	CaseTitle, The title of the case		String	MJ (ADJAJ)	PIGD	MConnect
5.6	CaseType	CaseType, The type of the case: 1 - Civil; 2 - Criminal; 3 - Contravenional		Integer	MJ (ADJAJ)	PIGD	MConnect
5.7	Category	Category, The category of the case		Category	MJ (ADJAJ)	PIGD	MConnect
5.8	Court	Court, The unique identifier of the court		String	MJ (ADJAJ)	PIGD	MConnect

ID	Field	Description	Required	Format	Institution	System	Integration
5.9	ExaminationType	ExaminationType, The type of examination. Contains values from the ExaminationType classifier		Integer	MJ (ADJAJ)	PIGD	MConnect

5. Reference Data Assets from the Semantic Catalog

The following governmental data assets and semantic schemas are identified as reference points for field mapping:

ID	Catalog Data Set Name	Link
1	Persons with disabilities	https://semantic.gov.md/ro/assets/details/079b193d-85c5-4a42-8030-5314571b31b5
2	GetPersonCases	https://semantic.gov.md/ro/assets/details/4e263ca7-7c1d-4134-aa19-593267f944fe
3	Place of detention	https://semantic.gov.md/ro/assets/details/33037ebb-9c9c-40df-b300-58824236ff66
4	Detention status	https://semantic.gov.md/ro/assets/details/6a937390-3a50-47f1-bb2f-d38ac9c69660
5	Cases	https://semantic.gov.md/ro/assets/details/f25f9f4e-d610-466d-8c06-b7f737907f0c
6	Natural person	https://semantic.gov.md/en/assets/details/17e78ff1-a169-4359-9fa4-c055496c9c1f
7	Documents	https://semantic.gov.md/ro/assets/details/800b3940-79db-4ba9-9f60-8dc8ecc49853
8	Document type	https://semantic.gov.md/ro/assets/details/c5cc4812-5a34-4a2a-9a9a-2d1f1263d494
9	Address	https://semantic.gov.md/ro/assets/details/7e338d81-65cf-43b6-bbf6-71abb7df560d
10	Localities	https://semantic.gov.md/ro/assets/details/d56035b0-7d24-45cd-9962-417bcb5e08a9

ID	Catalog Data Set Name	Link
11	Citizenship	https://semantic.gov.md/ro/assets/details/a056a4b8-89a8-4680-9a0d-4fb9fccd5c2f
12	Document type	https://semantic.gov.md/ro/assets/details/c5cc4812-5a34-4a2a-9a9a-2d1f1263d494
13	Status or reason for updating document status	https://semantic.gov.md/ro/assets/details/fa6b4c77-cc7d-4582-8546-373f691d324e
14	GetOrganizationDataRSUD2	https://semantic.gov.md/ro/assets/details/c5fe35e2-536b-44f2-afa8-5aae7c8a607b
15	Classifier of Administrative-Territorial Units of the Republic of Moldova (CUATM)	https://semantic.gov.md/ro/assets/details/05dd4d35-334d-4bd7-a751-c8b2d099c6e4

SECTION 6: CONDITIONS OF CONTRACT AND CONTRACT FORMS

6.1 The types of Contract to be signed and the **applicable UNDP Contract General Terms and Conditions**, as specified in Data Sheet, can be accessed at http://www.undp.org/content/undp/en/home/procurement/business/how-we-buy.html

6.2 Special Conditions of Contract
N/A

SECTION 7: PROPOSAL FORMS

- **Form A: Proposal Confirmation**
- **Form B: Checklist**
- **Form C: Technical Proposal Submission**
- **Form D: Proposer Information**
- **Form E: Joint Venture/Consortium/Association Information**
- **Form F: Eligibility and Qualification**
- **Form G: Format for Technical Proposal**
- **Form H: Format for CV of Proposed Key Personnel**
- **Form I: Statement of Exclusivity and Availability**
- **Form J: Financial Proposal Submission** *[Form J is part of the Financial Proposal and shall be submitted directly in the system only in the "Commercial section" of the requirements. Please, ensure that no other documents are disclosing your financial proposal apart from Forms J and K. Non-compliance with this instruction may result in rejection of the proposal received.]*
- **Form K: Format for Financial Proposal** *[Forms K is part of the Financial Proposal and shall be submitted directly in the system only in the "Commercial section" of the requirements. Please, ensure that no other documents are disclosing your financial proposal apart from Forms J and K. Non-compliance with this instruction may result in rejection of the proposal received.]*
- **Form L: Proposal Security** *[scanned copy included in online submission and original submitted not later than 10 (ten) days after the submission deadline at the address indicated in Section 3 above]*

FORM A: PROPOSAL CONFIRMATION

Please acknowledge receipt of this RFP by completing this form and returning it by email to the address, and by the date specified, in the Letter of Invitation.

To: Insert name of contact person Email: Insert contact person's email - do not enter secure proposal email address

From: Insert name of proposer

Subject RFP reference Click or tap here to enter text.

Check the appropriate box	Description
☐	**YES**, we intend to submit a proposal.
☐	**NO**, we are unable to submit a competitive proposal for the requested services at the moment

If you selected NO above, please state the reason(s) below:

Check applicable	Description
☐	The requested services are not within our range of supply
☐	We are unable to submit a competitive proposal for the requested services at the moment
☐	The requested services are not available at the moment
☐	We cannot meet the requested terms of reference
☐	The information provided for proposal purposes is insufficient
☐	Your RFP is too complicated
☐	Insufficient time is allowed to prepare a proposal
☐	We cannot meet the delivery requirements
☐	We cannot adhere to your terms and conditions e.g. payment terms, request for performance security, etc. Please provide details below.
☐	Sustainability criteria/requirements are too stringent (if applicable)
☐	We do not export
☐	We do not sell to the UN
☐	Your requirement is too small
☐	Our capacity is currently full
☐	We are closed during the holiday season
☐	We had to give priority to other clients' requests
☐	The person handling proposals is away from the office
☐	Other (please provide reasons below):
Further information: Click or tap here to enter text.	
☐	We would like to receive future RFPs for this type of services
☐	We don't want to receive RFPs for this type of services

Questions to the Supplier concerning the reasons for no proposal should be addressed to Click or tap here to enter text. phone Click or tap here to enter number., email Click or tap here to enter text..

FORM B: CHECKLIST

This form serves as a checklist for preparation of your Proposal. Please complete the returnable Proposal Forms in accordance with the instructions and return them as part of your Proposal submission: No alteration to the format of forms shall be permitted and no substitution shall be accepted.
Before submitting your Proposal, please ensure compliance with the instructions in Section 2: Instructions to Proposers and Section 3: Data Sheet.

Technical Proposal:

Have you duly completed all the Returnable Proposal Forms?	
Form C: Technical Proposal Submission	☐
Form D: Proposer information	☐
Form E: Joint Venture/Consortium/Association Information	☐
Form F: Eligibility and Qualification	☐
Form G: Technical Proposal	☐
Form H: CVs of proposed key personnel	☐
Form I: Statements of exclusivity and availability for key personnel	☐
Form L: Proposal Security *[scanned copy included in online submission and original submitted not later than 10 (ten) days after the submission deadline at the address indicated in Section 3 above]*	☐
Have you provided the required documents to establish compliance with the evaluation criteria in Section 4?	☐
Have you provided the required documents in support of Form D: Proposer Information?	☐

Financial Proposal:

Form J: Financial Proposal Submission	☐
Form K: Financial Proposal	☐

Forms J and K, representing the Financial Proposal shall be submitted directly in the system only in the "Commercial section" of the requirements. Please, ensure that no other documents are disclosing your financial proposal apart from Forms J and K. Non-compliance with this instruction may result in rejection of the proposal received.

FORM C: TECHNICAL PROPOSAL SUBMISSION

Name of Proposer:	Click or tap here to enter text.	Date:	Click or tap to enter a date.
RFP reference:	Click or tap here to enter text.		

We, the undersigned, offer to supply the services required for Click or tap here to enter text.in accordance with your Request for Proposals No. Click or tap here to enter text.. We hereby submit our Proposal, which includes this Technical Proposal and our Financial Proposal uploaded separately under the commercial section in the system as instructed.

Proposer Declaration: on behalf of our firm, its affiliates, subsidiaries and employees, including any JV / Consortium / Association members or subcontractors or suppliers for any part of the contract.

Yes	No	
☐	☐	**Requirements and Terms and Conditions:** I/We have read and fully understand the RFP, including the RFP Information and Data Sheet, Terms of Reference, the General Conditions of Contract and any Special Conditions of Contract. I/we confirm that the proposer agrees to be bound by them.
☐	☐	I/We confirm that the proposer has the necessary capacity, capability and necessary licenses to fully meet or exceed the requirements and will be available to deliver throughout the relevant contract period.
☐	☐	**Ethics**: In submitting this proposal I/we warrant that the proposer: has not entered into any improper, illegal, collusive or anti-competitive arrangements with any competitor; has not directly or indirectly approached any representative of the buyer (other than the point of contact) to lobby or solicit information in relation to the RFP; has not attempted to influence, or provide any form of personal inducement, reward or benefit to any representative of the buyer.
☐	☐	I/We confirm to undertake not to engage in proscribed practices, or any other unethical practice, with the UN or any other party, and to conduct business in a manner that averts any financial, operational, reputational or other undue risk to the UN and we have read the United Nations Supplier Code of Conduct :https://www.un.org/Depts/ptd/about-us/un-supplier-code-conduct and acknowledge that it provides the minimum standards expected of suppliers to the UN.
☐	☐	**Conflict of interest:** I/We warrant that the proposer has no actual, potential or perceived conflict of Interest in submitting this proposal, or entering into a contract to deliver the requirements. Where a conflict of interest arises during the RFP process the proposer will report it immediately to the Procuring Organisation's Point of Contact.
☐	☐	**Prohibitions and Sanctions:** I/We hereby declare that our firm, ultimate beneficial owners, affiliates or subsidiaries or employees, including any JV/Consortium members or subcontractors or suppliers for any part of the contract is not under procurement prohibition by the United Nations, including but not limited to prohibitions derived from the Compendium of United Nations Security Council Sanctions Lists and have not been suspended, debarred, sanctioned or otherwise identified as ineligible by any UN Organization or the World Bank Group or any other international Organization.
☐	☐	I/We do not employ, or anticipate employing, any person(s) who is, or has been a UN staff member within the last year, if said UN staff member has or had prior professional dealings with our firm in his/her capacity as UN staff member within the last three years of service with the UN (in accordance with UN post-employment restrictions published in ST/SGB/2006/15);
☐	☐	**Bankruptcy**: I/We have not declared bankruptcy, are not involved in bankruptcy or receivership proceedings, and there is no judgment or pending legal action against us that could impair our operations in the foreseeable future.

Yes	No	
☐	☐	**Proposal Validity Period:** I/We confirm that this Proposal, including the price, remains open for acceptance for the proposal validity period.
☐	☐	I/We understand and recognize that you are not bound to accept any proposal you receive.
☐	☐	By signing this declaration, the signatory below represents, warrants and agrees that he/she has been authorised by the Organisation/s to make this declaration on its/their behalf.

Name: _____
Title: _____
Date: _____
Signature: _____
[*Stamp with official stamp of the Proposer*]

FORM D: PROPOSER INFORMATION

RFP Reference	Click or tap here to enter text.
Legal name of Proposer	Click or tap here to enter text.
Legal Address, City, Country	Click or tap here to enter text.
Website	Click or tap here to enter text.
Year of registration	Click or tap here to enter text.
Proposer's Authorized Representative information	Name and Title: Click or tap here to enter text. Telephone numbers: Click or tap here to enter text. Email: Click or tap here to enter text.
Legal structure	Choose an item.
No. of full-time employees	Click or tap here to enter number.
No. of staff involved in similar contracts	Click or tap here to enter number.
Are you a UNGM registered vendor?	☐ Yes ☐ No If yes, insert UNGM Vendor Number
Years of supplying to UN organisations	Click or tap here to enter text.
Are you a UNDP vendor?	☐ Yes ☐ No If yes, insert Vendor Number
Countries of operation	Click or tap here to enter text.
Subsidiaries in the region (please indicate names of subsidiaries and addresses, if relevant to the proposal)	Click or tap here to enter text.
Commercial Representatives in the country: Name/Address/Phone (for international companies only)	Click or tap here to enter text.
Quality Assurance Certification (e.g. ISO 9000 or Equivalent) *(If yes, provide a Copy of the valid Certificate):*	Click or tap here to enter text.
Does your Company have a corporate environmental policy or environmental management system/accreditation such as ISO 14001 or ISO 14064 or equivalent? *(If yes, provide a Copy of the valid Certificate):*	Tick all that apply and **provide supporting documentation**: ☐ Corporate Environmental Policy ☐ ISO 14001 ☐ ISO 14064 ☐ Other, specify Click or tap here to enter text.
Does your organization demonstrate significant commitment to sustainability, including the following aspects that have been identified in the UN Sustainable Procurement Framework? **Environmental: prevention of pollution, sustainable resources; climate change and mitigation and the protection of the environment, biodiversity.** **Social: human rights and labour issues, gender equality, sustainable consumption, and social health and wellbeing.**	Attach a formal statement that outlines your organisation's commitment to sustainability, where possible providing evidence of tangible results that demonstrate progress such as: Tick all that are attached: ☐ Formal statement ☐ Sustainability report ☐ UN Global Compact Communication on Progress ☐ Other, specify Click or tap here to enter text.

Economic: whole life cycle costing, local communities and small or medium enterprises, and supply chain sustainability.	
Does your company belong to a diverse supplier group including micro, small or medium sized enterprise, women or youth owned business or other? *(If yes, please provide details and documentation]*	Click or tap here to enter text.
Is your company a member of the UN Global Compact?	Choose an item. If yes, please provide link to Global Compact profile: Click or tap here to enter text.
Bank Information	Bank Name: Click or tap here to enter text. Bank Address: Click or tap here to enter text. IBAN: Click or tap here to enter text. SWIFT/BIC: Click or tap here to enter text. Account Currency: Click or tap here to enter text. Bank Account Number: Click or tap here to enter text.
Contact person that Click or tap here to enter text. **may contact for requests for clarifications during Proposal evaluation**	Name and Title: Click or tap here to enter text. Telephone numbers: Click or tap here to enter text. Email: Click or tap here to enter text.

FORM E: JOINT VENTURE/CONSORTIUM/ASSOCIATION INFORMATION

Name of Proposer:	Click or tap here to enter text.	Date:	Click or tap to enter a date.
RFP reference:	Click or tap here to enter text.		

To be completed and returned with your Proposal if the Proposal is submitted as a Joint Venture/Consortium/Association.

No	**Name of Partner and contact information** *(address, telephone numbers, fax numbers, e-mail address)*	**Proposed proportion of responsibilities (in %) and type of services to be performed**
1	Click or tap here to enter text.	Click or tap here to enter text.
2	Click or tap here to enter text.	Click or tap here to enter text.
3	Click or tap here to enter text.	Click or tap here to enter text.

Name of leading partner (with authority to bind the JV, Consortium, Association during the RFP process and, in the event a Contract is awarded, during contract execution)	Click or tap here to enter text.

We have attached a copy of the below referenced document signed by every partner, which details the likely legal structure of and the confirmation of joint and severable liability of the members of the said joint venture:

☐ Letter of intent to form a joint venture ***OR*** ☐ JV/Consortium/Association agreement

We hereby confirm that if the contract is awarded, all parties of the Joint Venture/Consortium/Association shall be jointly and severally liable to Click or tap here to enter text for the fulfilment of the provisions of the Contract.

Name of partner: _____

Signature: _____

Date: _____

Name of partner: _____

Signature: _____

Date: _____

Name of partner: _____

Signature: _____

Date: _____

Name of partner: _____

Signature: _____

Date: _____

FORM F: ELIGIBILITY AND QUALIFICATION

Name of Proposer:	Click or tap here to enter text.	Date:	Click or tap to enter a date.
RFP reference:	Click or tap here to enter text.		

If JV/Consortium/Association, to be completed by each partner.

History of Non- Performing Contracts

☐No non-performing contracts during the last 3 years			
☐ Contract(s) not performed in the last 3 years			
Year	**Non- performed portion of contract**	**Contract Identification**	**Total Contract Amount** (current value in US$)
		Name of Client: Address of Client: Reason(s) for non-performance:	

Litigation History (including pending litigation)

☐ No litigation history for the last 5 years			
☐ Litigation History as indicated below			
Year of dispute	**Amount in dispute** (state currency)	**Contract Identification**	**Total Contract Amount** (state currency)
		Name of Client: Address of Client: Matter in dispute: Party who initiated the dispute: Status of dispute: Party awarded if resolved:	

Previous Relevant Experience

Please list only previous similar assignments successfully completed in the **last 5 years**.

List only those assignments for which the Proposer was legally contracted or sub-contracted by the Client as a company or was one of the Consortium/JV partners. Assignments completed by the Proposer's individual experts working privately or through other firms cannot be claimed as the relevant experience of the Proposer, or that of the Proposer's partners or sub-consultants, but can be claimed by the Experts themselves in their CVs. The Proposer should be prepared to substantiate the claimed experience by presenting copies of relevant documents and references if so requested.

Project name & Country of Assignment	**Client & Reference Contact Details**	**Contract Value**	**Period of activity and status**	**Types of activities undertaken and role (Contractor, sub-contractor or consortium member)**

Proposers may also attach their own Project Data Sheets with more details for assignments above.

☐ Attached are the Statements of Satisfactory Performance from the Top 3 (three) Clients or more.

Financial Standing

Annual sales Turnover for the last 3 years	**Year 2025**	Currency: USD	Amount

	Year 2024	Currency: USD	Amount
	Year 2023	Currency: USD	Amount
Latest Credit Rating (if any), indicate the source and date.			

Financial information (state currency)	**Historic information for the last 3 years**		
	2025	**2024**	**2023**
	Information from Balance Sheet		
Total Assets (TA)			
Total Liabilities (TL)			
Current Assets (CA)			
Current Liabilities (CL)			
	Information from Income Statement		
Total / Gross Revenue (TR)			
Profits Before Taxes (PBT)			
Net Profit			
Current Ratio (current assets/current liabilities)			

☐ Attached are copies of the audited financial statements (balance sheets, including all related notes, and income statements) for the years required above complying with the following condition:

a) Must reflect the financial situation of the Proposer or party to a JV, and not sister or parent companies;
b) Historic financial statements must be audited by a certified public accountant;
c) Historic financial statements must correspond to accounting periods already completed and audited. No statements for partial periods shall be accepted.

FORM G: FORMAT FOR TECHNICAL PROPOSAL

Name of Proposer:	Click or tap here to enter text.	Date:	Click or tap to enter a date.
RFP reference:	Click or tap here to enter text.		

The proposer's proposal must be organised to follow the format of this Technical Proposal Form. Where the proposer is presented with a requirement or asked to use a specific approach, the proposer must not only state its acceptance, but also describe, where appropriate, how it intends to comply. Where a descriptive response is requested, failure to provide the same will be viewed as non-responsive.

Section 1: Proposer's qualification, capacity and expertise

1.1 Brief description of the organisation, including the year and country of incorporation, and types of activities undertaken.

1.2 General organizational capability which is likely to affect implementation: management structure, financial stability and project financing capacity, project management controls, extent to which any work would be subcontracted (if so, provide details).

1.3 Relevance of specialised knowledge and experience on similar engagements done in the region/country.

1.4 Quality assurance procedures and risk mitigation measures.

1.5 Organization's commitment to sustainability.

Section 2: Proposed Methodology, Approach and Implementation Plan

This section should demonstrate the proposer's responsiveness to the TOR by identifying the specific components proposed, addressing the requirements, providing a detailed description of the essential performance characteristics proposed and demonstrating how the proposed approach and methodology meets or exceeds the requirements. All important aspects should be addressed in sufficient detail and different components of the project should be adequately weighted relative to one another.

2.1 A detailed description of the approach, conceptual framework and methodology for how the Proposer will achieve or exceed the requirements of the Terms of Reference, keeping in mind the appropriateness to local conditions and project environment. Detail how the different service elements shall be organised, controlled and delivered.

2.2 A detailed description of the Bidder's internal technical and quality assurance mechanisms and risks identified, if any.

2.3 A detailed description of the System's technical functional and non-functional requirements.

2.4 Implementation plan including a Gantt chart or Project Schedule indicating the detailed sequence of activities that will be undertaken and their corresponding timing.

2.5 Any other comments or information regarding the project approach and methodology that will be adopted.

Section 3: Management Structure and Key Personnel

3.1 Describe the overall management approach toward planning and implementing the project. Include details of key personnel including their name and nationality, the Position they will assume and their role as per the ToR. Include an organisation chart for the management of the project describing the relationship of key positions and designations. Provide a spreadsheet to show the activities of each personnel and the time allocated for his/her involvement.

3.2 For each of the key personnel provide: the CV using the format in **Form H** and the statement of exclusivity and availability using the format in Form I. *Please provide copies of Certifications/Awards for the Key Personnel to be involved in the project.*

FORM H: FORMAT FOR CV OF PROPOSED KEY PERSONNEL

Name of Proposer:	Click or tap here to enter text.	Date:	Click or tap to enter a date.
RFP reference:	Click or tap here to enter text.		

Position (as per ToR)		
Personnel Information	Name:	
	Nationality:	Date of birth:
	Language Proficiency:	
Present Employment	Name of employer:	Contact: (manager or HR)
	Address of employer:	
	Telephone:	Email:
	Job title:	Years with present employer:
Education / Qualifications	*Summarise college/university and other specialised education of personnel member, giving names of schools, dates attended, and degrees/qualifications obtained.*	
Professional Certifications	*Provide details of professional certifications relevant to the scope of services including name of institution and date of certification.*	
References:	*Provide names, addresses, phone and email contact information for two (2) references*.	

Summarise professional experience over the last 20 years in reverse chronological order. Indicate particular technical and managerial experience relevant to the project.

From	To	Company / Project / Position / Relevant technical and management experience

I, the undersigned, certify that, to the best of my knowledge and belief, this CV is accurate.
Signature of Personnel Data (Day/Month/Year)

_____

_____

FORM I: STATEMENT OF EXCLUSIVITY AND AVAILABLITY

Name of Proposer:	Click or tap here to enter text.	Date:	Click or tap to enter a date.
RFP reference:	Click or tap here to enter text.		

I, the undersigned, hereby declare that I agree to participate exclusively with the Proposer Click or tap here to enter text.in the above referenced RFP. I further declare that I am able and willing to work for the period(s) foreseen for the position for which my CV has been included in the event that this proposal is successful, namely:

From	**To**
Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.

I confirm that I am not engaged in other projects in a position for which my services are required during the periods where my services are required under this RFP.

By making this declaration, I understand that I am not allowed to present myself as a candidate to any other proposer submitting a proposal for this RFP. I am fully aware that if I do so, I will be excluded from this RFP, the proposals may be rejected, and I may also be subject to exclusion from other UNDP's solicitation procedures and contracts.

Furthermore, should this proposal be successful, I am fully aware that if I am not available at the expected start date of my services for reasons other than ill-health or *force majeure*, I may be subject to exclusion from other Click or tap here to enter text. solicitation procedures and contracts and that the notification of award of contract to the Proposer may be rendered null and void.

Name: _____

Title: _____

Date: _____

Signature: _____

FORM J: FINANCIAL PROPOSAL SUBMISSION

Name of Proposer:	Click or tap here to enter text.	Date:	Click or tap to enter a date.
RFP reference:	Click or tap here to enter text.		

We, the undersigned, offer to provide the services indicated in our proposal and in accordance with your Request for Proposal. We are hereby submitting our Financial Proposal in the amount indicated herewith.

Our Proposal shall be valid and remain binding upon us for the period of time specified in the Data Sheet.

We understand that you are not bound to accept any Proposal that you receive.

Our attached Financial Proposal is for the sum of *[Insert amount in words and figures]*. Please make sure the total matches with the total indicated in the deliverables section of the system (lines) and with the total deriving from the cost breakdown (form K).

FORM K: FORMAT FOR FINANCIAL PROPOSAL

Name of Proposer:	Click or tap here to enter text.	Date:	Click or tap to enter a date.
RFP reference:	Click or tap here to enter text.		

The proposer is required to prepare the Financial Proposal following the below format and submit it in an envelope separate from the Technical Proposal as indicated in the Instruction to Proposers. **The inclusion of any financial information in the Technical Proposal shall lead to disqualification of the Proposer.**

The Financial Proposal should align with the requirements of the Terms of Reference and the proposer's Technical Proposal. **Currency of the proposal: MDL (Moldovan Leu) for local suppliers and USD (US Dollars) for international suppliers, VAT exclusive**

Table 1 Financial Proposal:

Deliverable / Activity description	Professional Fees				Other Costs				Total Amount per deliverable (subtotal 1 + sub-total 2)
	Position	Daily fee Rate	No. of Working Days	Total Amount	Description	Q-ty	Price	Total	
Activity 1: Kick off meeting with the CEC and the UNDP Project Team **Deliverable 1:** Detailed minutes of the meeting confirming the scope, approach and work plan – developed, submitted and approved by the CEC and UNDP Project Team	1 (one) Project Manager				Travel (if any)				
	1 (one) Business Analyst with Training responsibilities				Local transportation costs (if any)				
	1 (one) System Architect				Communication Expenses				
	1 (one) Team Leader and Senior Software Developer with UX/UI Coordination responsibilities				Other costs (please specify)				
	1 (one) Software Developer with Database Administration responsibilities								
	1 (one) Software Developer with DevOps responsibilities								
	1 (one) QA Expert								
	1 (one) Trainer / Training Expert								
	Other experts (if any) *[Please list]*								
			Sub-total 1				**Sub-total 2**		

Activity 2: Develop a detailed Project Implementation Plan **Deliverable 2:** Project Implementation Plan confirming the roles of stakeholders, focal points, deliverables, timeline, etc. – submitted and approved by CEC and UNDP Project Team	1 (one) Project Manager				Travel				
	1 (one) Business Analyst with Training responsibilities				Subsistence allowance				
	1 (one) System Architect				Local transportation costs				
	1 (one) Team Leader and Senior Software Developer with UX/UI Coordination responsibilities				Communication				
	1 (one) Software Developer with Database Administration responsibilities				Other costs (specify)				
	1 (one) Software Developer with DevOps responsibilities								
	1 (one) QA Expert								
	1 (one) Trainer / Training Expert								
	Other experts (if any) *[Please list]*								
			Sub-total 1				**Sub-total 2**		
								Total:	
Activity 3: Develop a detailed System Architecture Document of the computer subsystem 'State Registry of Voters' of State Automated Information System 'Elections' **Deliverable 3:** System Architecture Document, confirming the architecture and components, data architecture, technology stack, integrations and interfaces, non-functional requirements, deployment setup, operational considerations, etc. - submitted and approved by CEC and UNDP Project Team	1 (one) Project Manager				Travel (if any)				
	1 (one) Business Analyst with Training responsibilities				Local transportation costs (if any)				
	1 (one) System Architect				Communication Expenses				
	1 (one) Team Leader and Senior Software Developer with UX/UI Coordination responsibilities				Other costs (please specify)				
	1 (one) Software Developer with Database Administration responsibilities								
	1 (one) Software Developer with DevOps responsibilities								
	1 (one) QA Expert								

	1 (one) Trainer / Training Expert								
	Other experts (if any) *[Please list]*								
		Sub-total 1				**Sub-total 2**			
								Total:	
Activity 4: Develop the computer subsystem 'State Registry of Voters' of State Automated Information System 'Elections' **Deliverable 4:** Computer subsystem 'State Registry of Voters' of State Automated Information System 'Elections' fully developed in accordance with the approved System Architecture Document and technical specifications (Deliverable 3), including fully developed front-end and back-end, configured databases, implemented business logic, integrated interfaces with external systems. The subsystem should be functionally complete and integrated at information system level, deployed in the testing environment and demonstrated to CEC and UNDP Project Team	1 (one) Project Manager				Travel				
	1 (one) Business Analyst with Training responsibilities				Subsistence allowance				
	1 (one) System Architect				Local transportation costs				
	1 (one) Team Leader and Senior Software Developer with UX/UI Coordination responsibilities				Communication				
	1 (one) Software Developer with Database Administration responsibilities				Other costs (specify)				
	1 (one) Software Developer with DevOps responsibilities								
	1 (one) QA Expert								
	1 (one) Trainer / Training Expert								
	Other experts (if any) *[Please list]*								
		Sub-total 1				**Sub-total 2**			
								Total:	
Activity 5: Preparation of Test Plans for the computer subsystem 'State Registry of Voters' of State Automated Information System 'Elections' **Deliverable 5:** Test plans for User Acceptance Testing, Load & Stress Testing and Automation Testing Plans, including the strategy, scope, approach, resources,	1 (one) Project Manager				Travel				
	1 (one) Business Analyst with Training responsibilities				Subsistence allowance				
	1 (one) System Architect				Local transportation costs				
	1 (one) Team Leader and Senior Software Developer with UX/UI Coordination responsibilities				Communicatio n				

schedule, etc. - completed and validated by the CEC and UNDP Project Team	1 (one) Software Developer with Database Administration responsibilities				Other costs (specify)				
	1 (one) Software Developer with DevOps responsibilities								
	1 (one) QA Expert								
	1 (one) Trainer / Training Expert								
	Other experts (if any) *[Please list]*								
			Sub-total 1				**Sub-total 2**		
								Total:	
Activity 6: Execute testing to verify functionality, performance, and compliance with requirements **Deliverable 6:** Assisted testing conducted with all type of users and detailed report proving that the system has been tested and issues have been addressed - reported and validated by to the CEC and UNDP Project Team	1 (one) Project Manager				Travel				
	1 (one) Business Analyst with Training responsibilities				Subsistence allowance				
	1 (one) System Architect				Local transportation costs				
	1 (one) Team Leader and Senior Software Developer with UX/UI Coordination responsibilities				Communication				
	1 (one) Software Developer with Database Administration responsibilities				Other costs (specify)				
	1 (one) Software Developer with DevOps responsibilities								
	1 (one) QA Expert								
	1 (one) Trainer / Training Expert								
	Other experts (if any) *[Please list]*								
			Sub-total 1				**Sub-total 2**		
								Total:	
Activity 7: Training for Users	1 (one) Project Manager				Travel				

Deliverable 7: 7.1. User manual, System installation and configuration manual, API integration guide and samples, Training materials – developed and presented to the CEC and UNDP Project Team 7.2. At least 2 user training sessions for CEC (the CEC will provide the necessary arrangements and logistics for organizing the training) – conducted and post training report submitted to the CEC and UNDP Project Team	1 (one) Business Analyst with Training responsibilities				Subsistence allowance				
	1 (one) System Architect				Local transportation costs				
	1 (one) Team Leader and Senior Software Developer with UX/UI Coordination responsibilities				Communication				
	1 (one) Software Developer with Database Administration responsibilities				Other costs (specify)				
	1 (one) Software Developer with DevOps responsibilities								
	1 (one) QA Expert								
	1 (one) Trainer / Training Expert								
	Other experts (if any) *[Please list]*								
			Sub-total 1				**Sub-total 2**		
								Total:	
Activity 8: Implementation the computer subsystem 'State Registry of Voters' of State Automated Information System 'Elections' **Deliverable 8:** 8.1. The system successfully configured and deployed in the Production Environment in compliance with all TOR requirements, with no critical or high-severity unresolved defects, evidenced by a Formal Acceptance Certificate validated by the CEC confirming successful commissioning. 8.2. Source Code and deployment documentation, System architecture and technical documentation, Security and testing documentation, User and	1 (one) Project Manager				Travel				
	1 (one) Business Analyst with Training responsibilities				Subsistence allowance				
	1 (one) System Architect				Local transportation costs				
	1 (one) Team Leader and Senior Software Developer with UX/UI Coordination responsibilities				Communication				
	1 (one) Software Developer with Database Administration responsibilities				Other costs (specify)				
	1 (one) Software Developer with DevOps responsibilities								

administrator guides – presented and delivered to the CEC and the UNDP Project Team. 8.3. Signed SLA covering the 12-months maintenance, warranty, and technical support services - formally approved by the CEC and UNDP Project Team	1 (one) QA Expert								
	1 (one) Trainer / Training Expert								
	Other experts (if any) *[Please list]*								
			Sub-total 1				**Sub-total 2**		
								Total:	
Activity 9: Maintenance, Warranty and Technical Support Services for 12-months following the commissioning of the system **Deliverable 9:** Report on Maintenance, Warranty and Technical Support Services for 12-months period following the system commissioning – formally approved by the CEC and the UNDP Project Team	1 (one) Project Manager				Travel				
	1 (one) Business Analyst with Training responsibilities				Subsistence allowance				
	1 (one) System Architect				Local transportation costs				
	1 (one) Team Leader and Senior Software Developer with UX/UI Coordination responsibilities				Communication				
	1 (one) Software Developer with Database Administration responsibilities				Other costs (specify)				
	1 (one) Software Developer with DevOps responsibilities								
	1 (one) QA Expert								
	1 (one) Trainer / Training Expert								
	Other experts (if any) *[Please list]*								
			Sub-total 1				**Sub-total 2**		
								Total:	
								TOTAL AMOUNT OF FINANCIAL PROPOSAL	

FORM L: PROPOSAL SECURITY

Proposal Security must be issued using the official letterhead of the Issuing Bank.

Except for indicated fields, no changes may be made on this template.

Beneficiary: Insert contact information for procuring organisation as provided in Section 3: Data Sheet.

RFP Reference: **RfP26/03301 Development of the computer subsystem "State Registry of Voters" of State Automated Information System "Elections"**

WHEREAS (hereinafter called "the Proposer") has submitted a Proposal to UNDP dated Click or tap to enter a date. to execute services Click or tap here to enter text. (hereinafter called "the Proposal"):

AND WHEREAS it has been stipulated by you that the Proposer shall furnish you with a Bank Guarantee by a recognized bank for the sum specified therein as security if the Proposer:

a) Fails to sign the Contract after UNDP has awarded it;
b) Withdraws its Proposal after the date of the opening of the Proposals;
c) Fails to comply with UNDP's variation of requirement, as per RFP instructions; or
d) Fails to furnish Performance Security, insurances, or other documents that UNDP may require as a condition torendering the contract effective.

AND WHEREAS we have agreed to give the Proposer such Bank Guarantee:

NOW THEREFORE we hereby affirm that we are the Guarantor and responsible to you, on behalf of the Proposer, up to a total of [*amount of guarantee*] [*in words and numbers*], such sum being payable in the types and proportions of currencies in which the Price Proposal is payable, and we undertake to pay you, upon your first written demand and withoutcavil or argument, any sum or sums within the limits of *[amount of guarantee as aforesaid*] without your needing to prove or to show grounds or reasons for your demand for the sum specified therein.

This guarantee shall be valid up to 30 days after the final date of validity of proposals.

SIGNATURE AND SEAL OF THE GUARANTOR BANK

Signature:_____
Name:_____
Title: _____
Date: _____
Name of Bank _____
Address_____

[Stamp with official stamp of the Bank]