EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR COMMUNICATIONS NETWORKS, CONTENT AND TECHNOLOGY

Online Platforms: Society
DSA Monitoring and Cooperation

European Commission

Call for tenders EC-CNECT/2025/OP/0095 - Design, Development and Deployment of Public-Facing Multilingual Chatbots to Support the Implementation of the Digital Services Act (DSA) and the Artificial Intelligence Act (AI Act)

Open procedure

TENDER SPECIFICATIONS

TABLE OF CONTENTS

1. SCOPE AND DESCRIPTION OF THE PROCUREMENT

1.1. Contracting authority: who is the buyer?

This call for tenders is launched and managed by the European Commission, DG CNECT - Communications Networks, Content and Technology, referred to as the contracting authority for the purposes of this call for tenders.

1.2. Subject: what is this call for tenders about?

This call for tenders concerns the design, development, piloting, delivery, and maintenance of two public-facing chatbots to support the implementation and enforcement of both the Digital Services Act (DSA) and Regulation (EU) 2024/1689 - the Artificial Intelligence Act (AI Act).

The DSA chatbot will provide users with information, guidance, and assistance on their rights under the DSA.

The AI Act chatbot will target small and medium-sized enterprises (SMEs), start-ups, and other stakeholders who may not have extensive legal or technical resources and are subject to the AI Act, offering guidance on key provisions, applicability, and compliance steps.

Both chatbots will be hosted on Commission's websites on the ec.europa.eu domain.

This initiative is structured with the objective of delivering a robust and operational solution while laying the groundwork for potential future scaling and reuse across other policy areas.

As part of the contract, maintenance shall include not only ensuring the continued availability and functionality of the system but also implementing regular security updates, vulnerability management, and the correction of bugs or errors that could impact performance or data protection.

1.3. Lots: is this call for tenders divided into lots?

This call for tenders is not divided into lots.

1.4. Description: what do we want to buy through this call for tenders?

The purchases that are the subject of this call for tenders, including any minimum requirements, are described in detail below.

Variants (alternatives to the model solution described in the tender specifications) are not allowed. The contracting authority will disregard any variants described in a tender.

1.4.1. Background and objectives

1.4.1.1. DSA chatbot

The Digital Services Act (DSA) – Regulation (EU) 2022/2065 – establishes a new framework for regulating online intermediaries and platforms across the European Union. It introduces harmonised rules to enhance user rights, ensure the accountability of digital services, and mitigate systemic risks

associated with online platforms. While the regulation imposes legal obligations on service providers, it also grants significant new rights to users and introduces transparency mechanisms that empower individuals, enforcement authorities, and civil society.

European Union citizens may face challenges in understanding and asserting their rights, and navigating platform-level complaint procedures. The chatbot will guide users in understanding and exercising their rights under the DSA.[1]

In this context, the objective of the contract is to design, develop, and deliver a multilingual, web-based chatbot that provides users with accessible, actionable, and reliable information over the DSA. The DSA chatbot will therefore guide users (mainly citizens) through key concepts, provide tailored procedural advice, and support real-world engagement with platforms and authorities. It will also provide users with information on how to access and use the DSA Transparency Database.

Beyond legal explanations of the DSA, the chatbot shall illustrate its practical benefits for citizens by showing how platforms have adapted — for instance, easier reporting tools, clearer explanations when content is removed, new redress mechanisms, or opt-out options from recommender systems. These examples should highlight the concrete improvements users experience as a result.

1.4.1.2. AI chatbot

In parallel, the contract also includes the development of a chatbot to support the implementation of the AI Act, with a particular focus on small and medium-sized enterprises (SMEs), start-ups, and other stakeholders who may not have extensive legal or technical resources.

This AI Act chatbot will help SMEs, start-ups, and other stakeholders understand the provisions of the regulation and will provide tailored, practical guidance on its application, including the classification of AI systems (e.g. high-risk vs. limited-risk), the different obligations and the implementation framework.

The objective is to lower the compliance barrier for innovators and facilitate responsible AI development and deployment in line with EU values. By translating the legal framework into accessible and actionable steps, the chatbot will support the uptake and enforcement of the AI Act across diverse sectors and Member States.

1.4.2. Detailed characteristics of the purchase

The contractor shall design, develop, and implement two chatbot solutions capable of providing EU citizens with clear, accessible, and accurate information about their rights and obligations under DSA, and offering SMEs and other entities subject to the AI Act practical guidance for understanding and complying with the AI Act. The content shall be presented in plain language, accessible to users with varying levels of digital literacy, and structured to enhance comprehension and usability.

In particular, the contractor shall design, develop, test, and deploy two chatbot solutions with the following functionalities:

[1] It will not provide information or outputs related to risk assessments under Articles 34/35 DSA.

1.4.2.1. Context-aware and linked support

The chatbots shall employ smart, context-aware assistance. They must:

- Tailor responses based on the nature of the query, platform type, and user location or language.
- Support intent recognition and dialogue management, by identifying the purpose behind user queries using simple, predefined categories, such as asking for information, reporting an issue, or requesting guidance. The chatbot can check with the user that the detected purpose is correct before continuing, to avoid misunderstandings or sending users to the wrong information.
- Apply layered navigation (e.g. progressive disclosure) to provide digestible content with the option for deeper exploration.
- Rely exclusively on official, verifiable EU sources (e.g. legal texts of the DSA and the AI Act, Commission guidance, implementing and delegated acts, etc.). This means that all content that is fed into the chatbot, notably as training data, must be reproduced from verifiable EU sources which are publicly available and be either copyright-free, protected by EU-owned copyright or licensed to the EU under terms that do not limit use of the licensed content to train artificial intelligence tools.
- Include terms of use determining the rules and disclaimers governing how users can interact with the chatbot. The terms of use should include, but not be limited to:
    - an explanation of the chatbot's purposes and it can and cannot do;
    - a limitation of liability for the European Commission;
    - information to users that they are interacting with an AI-based chatbot, not a human (to comply with the transparency obligations under the AI Act);
    - rules to prevent misuse of the chatbot;
    - explanation on how user data is processed, stored or shared;
    - a copyright notice with information regarding the owner of the chatbot's software, content and outputs.

This feature shall ensure that users receive accurate and situation-specific assistance without being overwhelmed by technical detail.

In the context of this chatbot, no profiling is performed, no automated decision-making producing legal or similarly significant effects takes place, and no evaluation of personal aspects is conducted. Nonetheless, in line with the transparency obligations set out in Article 15(2)(f) of Regulation (EU) 2018/1725, the privacy statement presented to users must clearly indicate the absence of such processing.

1.4.2.2. DSA Chatbot

❖ ***User rights under the DSA***

The DSA chatbot shall deliver structured, scenario-based explanations of core user rights under the DSA. This includes, but is not limited to:

- The right to report illegal content, such as hate speech, counterfeit goods, and fraudulent services. The chatbot shall reference the relevant legal provisions of the Digital Services Act (DSA), such as Article 16 (Notice and Action mechanisms) and Article 17 (Statement of Reasons), which enshrine these rights. The chatbot shall guide users on how to exercise this right on different types of platforms and clarify the process following content flagging.

- The right to receive clear and meaningful explanations from platforms regarding decisions to remove content or suspend accounts. The chatbot shall outline the obligations of platforms in this regard and specify applicable timeframes.
- The right to appeal platform decisions through internal mechanisms and independent out-of-court dispute settlement bodies. The chatbot shall describe both options, their applicable contexts, and documentation requirements.
- The right to opt out of profiling-based recommendations on VLOPs and VLOSEs. The chatbot shall explain how to deactivate such features and where to find the relevant settings on different platforms.

Where relevant, the chatbot shall highlight concrete changes introduced by platforms in response to these obligations, so that users can directly see the benefits (e.g. standardised reporting forms, transparent labels on ads, improved explanations of content moderation decisions).

Information shall be conveyed through interactive guidance, supported by use cases and step-by-step walkthroughs. The chatbot shall make legal concepts tangible and actionable.

❖ ***Safeguard against legal opinions and case-specific compliance evaluations***

The chatbot shall not provide, under any circumstance, an assessment, judgement, or opinion on whether a specific platform, service provider, or piece of conduct is in compliance with the Digital Services Act (DSA).

In particular, the chatbot must:

- Avoid individualised compliance assessments: e.g. questions such as *"Has [platform X] violated the DSA by removing my content?"* must be detected and handled as out-of-scope.
- Redirect appropriately: when receiving such queries, the chatbot shall inform the user politely that it cannot provide evaluations of legal compliance in individual cases, and guide them instead to the relevant rights, complaint mechanisms, or competent authorities (e.g. national Digital Services Coordinators).
- Stay strictly informational: responses must be limited to explaining relevant provisions of the DSA (e.g. Articles on notices and reasons, Article on risk assessments), describing user rights and available redress channels, and pointing to official sources (legislation, guidance, transparency database).

This safeguard shall be implemented through both (i) conversational design (dialogue flow including out-of-scope detection and redirection) and (ii) technical guardrails (intent recognition, filtering categories, refusal responses). The contractor shall document how these safeguards are implemented and tested during validation.

In addition, the contractor shall maintain flexibility to adjust the scope of responses if persona-based user journeys or user testing reveal a need for broader or different types of answers. Such adjustments must always be considered in close cooperation with the European Commission.

❖ ***Exercising user rights***

The chatbot shall provide dynamic, interactive workflows to support users in understanding and asserting their rights under the DSA. It shall guide users in navigating reporting, flagging, and complaint mechanisms offered by online platforms, with context-specific and actionable information tailored to the type of issue (e.g. hate speech, scams, misleading advertising), the platform involved (e.g. social media, marketplace, video-sharing, app store), and the user's Member State.

These workflows shall:

- Offer step-by-step guidance on how to report illegal content, submit complaints, and appeal moderation decisions using platform tools.
- Clarify internal vs. external redress mechanisms, including expectations around response timelines and outcomes.
- Assist users in preparing necessary information, such as relevant URLs, content descriptions, and justifications for notices or complaints.
- Provide examples or templates of structured messages or complaint forms (without enabling direct transmission through the chatbot).
- Offer tailored guidance on when and how to escalate issues to external bodies such as national Digital Services Coordinators in the cases foreseen by the DSA.
- Include links to platform-specific help centres, reporting tools, and national or EU-level redress bodies.
- Inform users about trusted flagger status and how this may affect the handling of flagged content.

This feature aims to improve user understanding, encourage responsible engagement with platform complaint mechanisms, and strengthen trust in the DSA's enforcement framework.

The chatbot shall not only guide users procedurally, but also underline what has improved compared to pre-DSA practices — for example, faster complaint handling, clearer escalation routes, and consistent information on appeal rights.

The chatbot will solely provide guidance and information; it is not legally binding and does not replace official channels, legal procedures, or centralised enforcement systems.

❖ ***Platform responsibilities under the DSA***

The chatbot shall explain the DSA's obligations imposed on online platforms, tailored to the provider's type and size:

- For Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs), the chatbot will provide general explanations of platform responsibilities under the DSA (e.g. obligations to provide statements of reasons, complaint mechanisms, trusted flaggers, transparency reporting). It will not cover systemic risk assessments or risk mitigation obligations under Articles 34/35. As mentioned above, the chatbot will not enter into any assessment of the VLOPs and VLOSEs compliance with the DSA nor will it present its explanations as legal advice or opinion.
- For small and medium-sized platforms, the chatbot shall explain baseline obligations such as maintaining a point of contact, providing clear terms and conditions, and implementing complaint mechanisms. As above, this should not be expressed in terms of legal or compliance assessment.

The chatbot shall illustrate differing obligations based on platform size and role, and present this information in a user-friendly, accessible manner. Explanations should, wherever possible, connect these obligations with the tangible benefits they bring for users (e.g. more predictable complaint handling, safer user environments, or more control over recommender systems).

❖ ***Transparency database***

The chatbot shall facilitate user access to transparency-related information made available under the DSA, as published in the European Commission's Transparency Database[2]. This includes structured data concerning content moderation decisions, online advertising, recommender systems, and systemic risk mitigation measures, particularly those reported by VLOPs and VLOSEs. The chatbot will only facilitate access to official transparency reports. It will not interpret or provide analysis of systemic risk mitigation measures reported therein.

The chatbot shall:

- Guide users to the Transparency Database established by the European Commission and explain its purpose, scope, and how it contributes to accountability under the DSA.
- Offer contextual guidance on how to interpret transparency data, including definitions of key terms, reporting obligations under the DSA, and what these indicators may mean for users, regulators, and civil society.
- Provide direct links to the relevant entries in the Transparency Database, as well as platform-published transparency reports, ensuring all references are official, verifiable, and up to date.

This feature shall support users in navigating the transparency ecosystem introduced by the DSA. In addition, the contractor shall explicitly analyse the feasibility of chatbot queries relating to the Transparency Database. Given that querying structured datasets differs from querying legal texts, the contractor must identify which types of queries are realistically answerable (e.g. pointing users to entries, explaining categories) and which are not (e.g. interpreting or analysing systemic risk data). The contractor must reflect on these limitations and propose mitigation approaches.

❖ ***Data collection for monitoring***

The chatbot shall collect, structure, and analyse anonymised and aggregated user interaction data. The sole purpose of this feature is to improve the usability of the chatbot and help the Commission understand recurring user needs or difficulties in navigating complaint and redress procedures under the DSA.

The chatbot shall:

- Capture high-level, anonymised statistics from user interactions, such as frequent topics, common questions, and recurring issues related to reporting mechanisms, appeals, or redress.
- Organise the data to enable trend analysis over time and highlight areas where users may need clearer guidance or additional support.
- Provide an analytics dashboard summarising aggregated trends and recurring user queries or confusion points, without directly reproducing any content that has been submitted to the chatbot by users.
- Allow for segmentation by relevant dimensions, such as platform type, issue category (e.g. scam, hate speech, disinformation), and geographical indicators (when available).

This feature is intended exclusively to improve guidance and user support. It shall not cover or generate insights related to the systemic risk assessment regime under Articles 34/35 DSA nor more in general any assessment concerning compliance with the DSA.

[2] https://transparency.dsa.ec.europa.eu/?lang=en

For transparency and compliance, the contractor shall clearly distinguish between:

- Initial collection of raw user interaction data, which may include technical metadata (e.g. IP address) required for localisation and analytics.
- Anonymisation procedures applied before any further processing, dashboard visualisation, or reporting.

1.4.2.3. AI Act Chatbot

❖ ***Purpose and Scope***

The AI Act chatbot shall provide clear answers to user questions about the AI Act. It will be trained on the Regulation, as well as relevant guidance and FAQs issued by the European Commission. Its core purpose is to support SMEs in understanding and applying their obligations under the AI Act.

❖ ***Key Features***

- Answer questions on the classification of AI systems by risk level (e.g. high-risk, limited-risk, prohibited).
- Provide explanations on transparency, documentation, human oversight, and post-market obligations.
- Clarify which obligations apply to different actors (e.g. providers, importers, distributors, deployers).
- Link to relevant official guidance documents or legal definitions where useful.

Information will be provided in a structured and accessible manner, tailored to the typical concerns of SMEs.

❖ ***Support Materials and Sources***

The chatbot shall guide users to authoritative sources, including:

- The AI Act Regulation text.
- Guidance, templates, and FAQs published by the European Commission and the AI Office.
- Relevant standardisation initiatives.

❖ ***Data Collection for Regulatory Insight***

The chatbot shall collect anonymised, high-level interaction data to identify common questions and areas of uncertainty. This will:

- Help the Commission understand where additional guidance is needed.
- Support the adaptive implementation of the AI Act.

The chatbot shall not collect any sensitive or business-confidential data. It will only capture anonymised, high-level interaction data (e.g. frequency of topics or common questions) to help the Commission identify areas where further guidance may be needed and to support the adaptive implementation of the AI Act.

1.4.2.4. Technical requirements

❖ ***General requirements***

The chatbot solutions shall meet the following minimum technical and functional requirements:

- Large Language Models (LLMs) and AI Frameworks: The chatbot must leverage state-of-the-art large language models (LLMs) to ensure accurate, relevant, and context-aware responses. Preference shall be given to European-developed LLMs (e.g. Mistral) where technically appropriate and legally viable, in line with the European Commission's digital sovereignty and open strategic autonomy objectives.
- Retrieval-Augmented Generation (RAG): The chatbot shall implement a retrieval-augmented generation (RAG) architecture, combining LLM-based generation with secure access to curated documents. The RAG framework must ensure:
  - Use of trusted and validated knowledge sources
  - Context-aware retrieval based on user queries
  - Dynamic updates to the knowledge base
  - Traceable references for factual grounding of responses
- Multilingual Support:
  - The chatbot must be fully functional in a selected set of official EU languages—focusing on those most widely used and best supported by existing LLMs, such as English, French, German, Spanish, Italian, Dutch, Portuguese, and Polish.
    The system must ensure high linguistic consistency, accurate legal and policy terminology, and full functional parity across these languages.
    (See also section 1.4.2.8: Performance, Accuracy, and Validation)
  - The chatbot must also be operational in all other official EU languages, even if with a lower level of linguistic refinement. Responses in these languages must still provide basic user assistance, be comprehensible, and meet accessibility standards. (See also section 1.4.2.8: Performance, Accuracy, and Validation)
- Natural Language Processing (NLP): The chatbot must support robust natural language understanding across supported languages. This includes:
  - Intent recognition
  - Entity extraction
  - Dialogue flow management
  - Context preservation across user sessions
- Knowledge Base Integration: The chatbot must be trained on a curated and updatable knowledge base containing:
  - Texts of the Digital Services Act (DSA) and Artificial Intelligence Act (AI Act)
  - Official guidance documents, FAQs, and implementation guidelines published by the European Commission
  - The system must support regular updates to reflect evolving legal interpretations, new regulatory developments, and changes in implementation practices.

❖ ***System compatibility***

In order to ensure full compatibility with the European Commission's existing and future on-premise infrastructure, the chatbot solutions must be developed using the Haystack framework (https://haystack.deepset.ai) for building pipelines and AI workflows. Haystack serves as the standard backend framework adopted by the Commission for AI-based chatbot deployments. This requirement

guarantees portability between cloud-based prototypes and on-premise hosting environments managed by the Commission.

In addition, if the contractor implements a semantic search or indexing component, the solution should use OpenSearch (https://opensearch.org/vector-search/) as the vector database, which is the default vector store used in the Commission's Haystack-compatible platform.

Furthermore, the contractor must design the back end using RESTful APIs. This ensures that any developed use cases or applications will remain portable and interoperable with the Commission's infrastructure.

The chatbot solutions must also support integration with the EU Login authentication mechanism to ensure compliance with the Commission's identity and access management policies.

Finally, the contractor shall ensure that the system is compatible with the Commission's Splunk security monitoring environment. All logs and relevant events must be exportable and structured in a way that allows integration with the EC Splunk instance for security and compliance purposes.

Compatibility with the Commission's Haystack-based deployments is a mandatory technical constraint. The contractor shall ensure that pipelines, indexing strategies, and workflow logic are natively compatible with this framework.

- ***Functional Features***

The chatbot must include specific user-facing features that ensure reliability, transparency, and a user-friendly experience aligned with the European Commission's standards.

- Escalation Option: The chatbot must include an escalation feature triggered when the user explicitly requests to speak to a human within the chat. This feature must be configurable and optional, depending on whether the European Commission decides to activate human escalation. When activated, it must ensure a reliable fallback to human assistance by redirecting the user to an appropriate contact point or form within the Commission's system. The chatbot must be able to detect escalation requests expressed in natural language (e.g. "I want to talk to someone", "Can I speak to a human?").
- Source Referencing: Every answer provided by the chatbot must include source references and links to the relevant legislation, official guidance, or validated Commission documentation. This is essential to ensure legal reliability, traceability, and to allow users to independently verify the information received.
- Customisable Personality: The chatbot must support the ability to customise tone, writing style, and answer structure to match the communication style required by the Commission. This includes the flexibility to adjust the chatbot's tone. The chatbot's LLM parameters, such as temperature, must be configured to minimise hallucinations and ensure controlled, consistent, and reliable responses.
- Scope Awareness and Out-of-Scope Handling: Both chatbots shall be designed to recognise and handle out-of-scope queries appropriately. When users submit questions that fall outside the scope of the Digital Services Act, the AI Act, or the competences of the European Commission, or outside the scope of the chat bot as identified above, the chatbot shall respond in a clear and polite manner, indicating that the request cannot be answered.

  In particular, the chatbot shall:

- Detect and flag queries that request individualised legal opinions or compliance assessments (e.g. *"Has [platform X] violated the DSA because they removed my content?"*).
- Provide appropriate redirection by informing the user that the chatbot cannot provide such evaluations and by guiding them to relevant rights, procedures, or competent authorities.
- Ensure that responses remain strictly informational (explanations of rights, obligations, and references to official sources) and display a disclaimer that the chatbot cannot replace legal advice or enforcement decisions.

- Voice Input Capability: The chatbot must support voice input functionality, allowing users to speak their queries directly into the interface. The system must reliably transcribe the voice input into text and generate a corresponding response. This feature shall be browser-compatible, respect accessibility requirements, and comply with the Commission's standards on IT security, data protection (EUDPR), and multilingual usability. The contractor shall ensure seamless integration of this capability during the development phase and test its performance across multiple languages.
- Continuous Learning and Feedback Integration: The chatbot must support a continuous learning process based on user feedback. This includes mechanisms for collecting user ratings on individual answers and flagging incorrect or incomplete responses. These features shall be designed to help fine-tune source prioritisation, improve answer quality, and guide future updates to the chatbot's retrieval and generation settings. Therefore, the contractor shall:
  - Map different user personas and develop user journeys for each, including hostile or malicious use-cases. This ensures that blind spots are avoided and that chatbot logic covers both expected and adversarial interactions.
  - Conduct structured user-testing during development with representatives of the identified personas. In addition, mechanisms for post-deployment feedback collection shall be built in, so that user groups can continuously provide input for improvements.

The contractor shall describe how these features will be technically implemented and provide examples of how each can be configured and maintained over time.

❖ *Back-end Architecture*

The contractor shall design a unified backend infrastructure supporting both chatbot applications (DSA and AI Act). The solution must include:

- A shared backend system with common services such as monitoring, security, authentication, and back-end user management.
- Two dedicated pipelines or instances, one for each chatbot, ensuring logical and operational separation between the DSA and AI Act components.
- Infrastructure that avoids unnecessary duplication while enabling efficient maintenance, scalability, and potential future integration with other Commission tools or systems.

Alternative architectural proposals may be accepted if tenderers provide a clear justification demonstrating equivalent or superior efficiency, scalability, and maintainability.

❖ *Front-end Integration*

The Commission is committed to making online information as accessible as possible to the largest possible number of users including those with visual, auditory, cognitive or physical disabilities, and those not having the latest technologies. The contractor will therefore observe the technical

requirements detailed in European accessibility standard EN 301 5493 , and the Web Content Accessibility Guidelines (WCAG)[4]. The target compliance level is WCAG 2.1, Level 'AA'.

The contractor will have to follow the rules applicable to Commission websites:

- Europa Web Guide including the design principles organising the European Commission web presence;
- Interinstitutional Style Guide;
- European Commission visual identity.

The chatbot must be fully compatible with the European Commission's web environment and seamlessly integrated into existing platforms.

- Drupal Compatibility: The chatbot must be easily integrable with the European Commission's Drupal-based websites. The contractor shall ensure that the chatbot is compatible with the Drupal content management system used across Commission web domains and that the integration does not disrupt site performance, structure, or accessibility standards.
- Commission Branding: The chatbot interface must fully comply with the European Commission's corporate visual identity and branding guidelines. This includes the design of the chatbot window, buttons, icons, and any other visible elements. The contractor must allocate sufficient design and development resources to ensure that the chatbot visually aligns with the hosting website and meets the Commission's communication standards.
- Device Compatibility: The chatbot must be fully compatible with both desktop and mobile interfaces, ensuring a consistent, responsive, and user-friendly experience across devices. The contractor shall ensure that the chatbot interface, functionality, and accessibility features are optimised for different screen sizes and input methods (e.g. keyboard, touch, mouse).

The chatbot must offer a monolingual interface in English, while providing responses in the user's selected language. The interface (e.g. chatbot window, menus, buttons) will remain in English, regardless of the response language. The contractor shall ensure that this configuration is fully functional and can easily accommodate language switching for the chatbot's answers.

The AI Act chatbot front-end will be hosted on the AI Act Single Information Platform, which will be a European Commission website on the ec.europa.eu domain serving as the central access point for information, guidance, and resources related to the AI Act.

❖ ***Hosting and Deployment***

The chatbot solution must be deployed using modern, flexible, and resilient infrastructure to ensure scalability, reliability, and long-term maintainability.

- Containerisation: The solution must be fully containerised using Docker or equivalent technologies to enable portable, efficient, and modular deployment. The contractor shall ensure that all system components can be managed and deployed in containers to facilitate updates, scaling, and potential migration across environments.
- Cloud Infrastructure: The hosting of the chatbot, including during the piloting stage and for internal releases, shall be carried out in a Cloud environment provided by the Cloud

[3] https://www.etsi.org/deliver/etsi_en/301500_301599/301549/03.02.01_60/en_301549v030201p.pdf

[4] https://www.w3.org/TR/WCAG21

infrastructure of the EU Institutions, in accordance with applicable security and data protection requirements.

- Resilience and Redundancy: The solution must include appropriate redundancy and failover mechanisms to ensure high availability and service continuity. The contractor shall deploy two dedicated and logically separated pipelines or instances, one for each chatbot, within a shared backend infrastructure. This architecture shall ensure that a failure affecting one chatbot does not impact the availability or functionality of the other.
- Scalability: The chatbot solution must scale to handle public EU-level usage. It should support at least 500 concurrent users and 5,000 queries per hour without degradation in response time or accuracy. The system must elastically scale to accommodate surges (e.g. legal deadlines, news coverage), with maximum response times of 2 seconds for initial interactions and 1.5 seconds for follow-ups. Performance must be consistent across all EU Member States, with minimum 99.5% monthly uptime. The contractor must describe the scaling and load balancing approach, and provide results of performance testing.

❖ ***Reporting and Analytics***

For each chatbot, the contractor shall deliver fully operational, built-in analytics and monitoring capabilities. These must include, at minimum:

- Integrated workspace and user analytics, providing essential usage metrics such as number of queries, most accessed topics, user navigation flows, and drop-off points.
- A ready-to-use, web-based analytics dashboard enabling the Commission to easily monitor chatbot performance and user engagement.
- Built-in options for generating periodic reports (e.g. monthly usage summaries, trend analyses) directly from the provided platform.
- Compatibility with established third-party monitoring tools (e.g. Langfuse, Weights & Biases, or equivalent) to support deeper analysis and monitoring is recommended.
- Configurable alerting features for detecting performance issues, abnormal usage patterns, or system errors.

The contractor shall detail how the reporting interface will be designed, updated, and maintained, and how reports will be accessible to the Commission.

❖ ***Security and Operational Safeguards***

The contractor must ensure that the chatbot solutions adhere to the highest standards of information security and are fully compliant with all security standards applicable to European Commission information systems, as outlined in the official documentation provided by DG DIGIT. This includes compliance with all relevant EU cybersecurity and data protection frameworks. These requirements must be applied across all phases of the chatbot lifecycle.

All security requirements must be defined, validated, and implemented before the delivery of the chatbot solution. The contractor shall engage with DG DIGIT, the Commission's Directorate-General for digital services, to carry out the necessary security assessments during development and prior to deployment.

The contractor shall host the chatbot in a cloud environment authorised by the EU institutions and ensure encryption of data in transit and at rest. The solution must include robust authentication and access control mechanisms for both frontend and backend systems, including integration with EU Login for authenticated access when required.

The chatbot must comply with the following core technical security measures:

- Protection against common web vulnerabilities, such as injection attacks, session hijacking, and cross-site scripting (XSS).
- Prevention of automated abuse and unauthorised content uploads.
- Antivirus scanning and secure storage of any uploaded content.
- Real-time security logging, audit trail mechanisms, and integration with the Commission's Security Information and Event Management (SIEM) solution (i.e. Splunk).
- Strong user management, including centralised Identity and Access Management (IAM) integration and secure user verification.

In addition, the chatbot must include guardrails and protections to prevent misuse and ensure safe and responsible operation:

Guardrails: Clearly defined response boundaries must prevent the generation of inappropriate, misleading, or irrelevant content. The chatbot must detect and block prompt injection or manipulation attempts.

Rate Limiting: The system must include query limits per IP address and session to prevent spamming and Denial-of-Service (DoS) attacks. Thresholds shall be proposed by the contractor and validated with the Commission.

❖ ***Legal and Compliance Guardrail***

The chatbot shall not provide assessments, opinions, or judgements on whether a specific online platform, provider, or conduct is in compliance with the Digital Services Act (DSA) or any other EU legislation. Queries such as *"Has [platform X] violated the DSA by removing my content?"* shall be treated as out-of-scope.

The contractor shall:

- Implement intent recognition and filtering mechanisms to detect such queries.
- Ensure the chatbot responds with a polite refusal, clearly informing the user that the chatbot cannot provide compliance evaluations in individual cases.
- Redirect the user towards relevant rights, complaint mechanisms, or competent authorities (e.g. national Digital Services Coordinators).
- Reinforce a general disclaimer that the chatbot only provides information on rights and obligations, and cannot replace legal advice, enforcement decisions, or formal complaint procedures.

This safeguard must be tested and validated as part of the accuracy and performance framework.

<u>AI-Specific Threat Protection</u>

- Prompt Injection Prevention: Implement multi-layered prompt injection detection and prevention mechanisms.
- Jailbreak Protection: Prevent attempts to bypass model safety guardrails and content policies.
- Model Manipulation Protection: Protect against attempts to manipulate model behaviour or extract sensitive information.
- Security Posture Assessment: Guardrail to detect and block OWASP top 10 threats on LLM.

RAG-Specific Security Controls

- Knowledge Base Security: Implement comprehensive security controls for RAG knowledge bases and vector databases.
- Retrieval Security and Access Control: Implement secure retrieval mechanisms with context-aware access controls.
- Vector Embedding Security: Protect vector embeddings from extraction, poisoning, and adversarial attacks.
- Document Source Validation: Validate and authenticate document sources to prevent poisoning and maintain data integrity.
- RAG-Specific Data Protection: Implement specialised data protection controls for RAG knowledge bases and retrieval processes.

Real-Time Monitoring and Threat Detection

- Behavioural Analytics: Implement advanced behavioural analytics for anomaly detection.
- Security Information and Event Management (SIEM) Integration: Provide comprehensive security event logging and SIEM integration.

Integration Requirements for Enterprise Environments

- Identity and Access Management (IAM) Integration: Integrate with EC identity systems for centralised access control.
- API Security and Management: Provide secure API access with comprehensive management capabilities.

Risk Management

- Risk Assessment: Provide comprehensive risk assessment capabilities for chatbot interactions.
- Incident Response and Management: Provide automated incident response capabilities with manual oversight options.
- Business Continuity and Resilience: Ensure business continuity through comprehensive resilience mechanisms.
- Security Posture Assessment: Continuously assess and report on overall security posture.

1.4.2.5. Data Protection and Privacy Requirements

The processing of personal data by the chatbot solution must comply with Regulation (EU) 2018/1725 (EUDPR).

Where the contractor processes personal data in the context of the present contract, the contractor must respect the EUDPR, including following instructions (in the light of Article 29 EUDPR) from the Commission. Where there are existing data protection records, the contractor will comply with these.

The chatbot must provide the technical capability to display a clear and accessible privacy statement at the start of the interaction.

The contractor will support the Commission in the drafting of the data protection record and privacy statement. The contractor will draft a Data Protection Risk Assessment and, if required, a Data Protection Impact Assessment (DPIA). Further information on the last two deliverables is provided under Section 1.4.3.6.

All hosting, storage, and handling of data must be carried out within the EU/EEA, with no personal data transferred to or accessed from outside this area under any circumstances, unless explicitly authorised by the European Commission and in full compliance with applicable data protection legislation. The contractor must implement appropriate technical and organisational safeguards to ensure compliance with this requirement, including contractual, technical, and monitoring measures that prevent any unauthorised access from outside the EU/EEA.

The chatbot must incorporate data protection by design and by default. The privacy statement shall clearly inform users about the automated nature of the system, any data collected, and confirm that no profiling or automated decision-making with legal or similar effects is carried out, as per Article 15(2)(f) EUDPR.

While the contractor is responsible for the design, development, and initial deployment of the chatbot solution, the European Commission will retain full operational control post-deployment. The chatbot shall be hosted within the EU Institutions' infrastructure, and only the Commission and its designated teams shall have access to collected data. No long-term operation or access to user interaction data shall be granted to the contractor beyond the scope of development, testing, and initial piloting.

Beyond empowering citizens, the chatbot will collect anonymised interaction data, with robust safeguards to prevent the collection, storage, or processing of any personal data. This data can help inform enforcement, detect emerging risks, and support future improvements in regulatory practice. Anonymisation will be implemented in line with applicable data protection legislation and recognised EU standards, and will be ensured through system-level design choices, including the exclusion of user identifiers, IP addresses, or session metadata, and by aggregating data at a level that makes individual tracing impossible. Regular verification, for example, through periodic reviews of methods used, sample testing to check for potential re-identification, and updates to techniques where necessary of anonymisation effectiveness must be carried out, and additional safeguards must be considered to address residual re-identification risks.

The contractor must ensure that raw data is stored temporarily and securely, is never accessible to unauthorised parties, and is irreversibly anonymised prior to any use for analytics or system improvement. These steps must be documented, and where a Data Protection Impact Assessment (DPIA) is required under Article 39 of Regulation (EU) 2018/1725, the contractor shall draft it under the supervision of the Commission.

In line with the defined scope, the chatbot will not process or analyse user queries for systemic risk monitoring purposes (Articles 34/35 DSA) nor more in general for the purpose of DSA compliance. Data collection will be strictly limited to improving the user experience with complaint navigation and rights' guidance.

1.4.2.6. Intellectual property

With respect to intellectual property, the contractor shall give particular consideration to Articles I.8 and I.11 of the special conditions and Article II.13 of the general conditions.

Under the above intellectual property (IP) regime, the contractor must obtain the necessary authorisations to use any pre-existing materials (as defined in the contract) protected by IP rights owned by third parties (e.g. icons, fonts, images, software libraries) and inform the contracting authority about such rights, in accordance with Articles I.8.3 and II.13.4 of the contract. In addition, the contractor must ensure that the rights of third parties to any materials included in the deliverables are correctly acknowledged (i.e., by indicating, as appropriate, the relevant source, copyright owner and conditions of reuse of the licensed material).

Pursuant to Section 1.4.2.1, all content that the contractor feeds into the chatbot must be reproduced from verifiable EU sources which are publicly available and be either copyright-free, protected by EU-owned copyright or licensed to the EU under terms that do not limit use of the licensed content to train artificial intelligence tools. In addition, as indicated under Section 1.4.3.6. the contractor is required to provide the contracting authority with a list of the sources of the content fed into the chatbot, with an indication of the respective copyright status and EU ownership or licence rights, i.e., (a) copyright-free/public domain; (b) copyright owned by the EU; or (c) licensed to the EU, with details regarding the specific licence.

In accordance with the provisions of the contract, the contractor guarantees that the deliverables, including the content fed into the chatbot and the output it generates when interacting with users, do not infringe third-party rights, including copyright.

For any development of open source software for the contracting authority, the contractor shall follow and implement the European Commission guidelines on *Legal Compliance in Developing Open Source Solutions*[5][1].

In particular, and even prior to handover, the contractor is expected to maintain a list of all direct and indirect dependencies of the produced code and any licenses related to these dependencies. This shall be accompanied where necessary by the indication of whether such dependencies have been modified via a software bill of materials. This list will be included in the source code and make explicit references to libraries and specific functions.

This is because the contracting authority may decide to make software developed under the contract available for reuse under an open-source license, in accordance with the Commission Decision of 8 December 2021 on open-source licensing and reuse of Commission software (2021/C 495 I/01). In that case, the contracting authority will determine the appropriate open-source license, in accordance with Article 5 of that Decision. Preference will be given to the European Union Public License (EUPL), to which end the contractor shall avoid the use of any incompatible licenses (i.e. licenses of products preventing subsequent distribution under EUPL). Any need for the incorporation or use of open-source materials under licenses that would restrict the contracting authority's ability to distribute any open-source artefacts under EUPL must be discussed in advance with the contracting authority, prior to any development, with a clear justification referring to available open-source options and technical constrains in the state of the art. The contracting authority and the contractor will then discuss available options. Use of any open-source materials that will impede distribution under EUPL will be agreed with the contracting authority.

1.4.2.7. Performance, Accuracy, and Validation

A performance, accuracy, and validation framework shall ensure the delivery of high-quality, multilingual, legally sound chatbot solutions that meet the European Commission's operational needs and public service standards.

The contractor shall ensure that the chatbots delivered under this contract meet rigorous performance, accuracy, and validation standards to guarantee legal robustness, user trust, and multilingual consistency.

[5] Available at guidelines/guideliness_contractors_legal_compliance_open_source.md · master · About Code Europa EU / About code.europa.eu · GitLab.

1.4.2.7.1. Performance and Accuracy Targets

- Legal Accuracy:
  - All chatbot answers must be legally accurate, consistent with the most recent and official EU sources, and fully aligned with the legal texts of the DSA, the AI Act, and related Commission guidance.
  - The European Commission will provide a reference list of questions and expected answers covering both the DSA and the AI Act to serve as a common validation dataset. This dataset shall be used throughout the testing phases to systematically assess chatbot accuracy, performance, and precision across all supported languages.
  - The Commission will make available internal experts for both the DSA and the AI Act to support the testing, validation, and accuracy review of the chatbot responses.
- Multilingual Performance:
  - The contractor shall ensure that the chatbot's response quality is consistently high across all EU official languages, with a target precision rate of at least 95% for languages well-supported by large language models (LLMs) (namely English, French, German, Spanish, Italian, Dutch, Portuguese, and Polish) and an average of at least 75% across all EU official languages, including smaller languages with more limited LLM support.
  - The contractor shall provide a multilingual test report demonstrating the precision rates per language, validated through a combination of automated testing and human review. The European Commission reserves the right to independently verify a representative sample of test cases before final acceptance.
  - Native-level validation by language experts is mandatory for all supported languages. The European Commission will provide access to internal native speaker experts to support the validation and testing process, including smaller languages. The contractor is expected to cooperate closely with these experts to ensure linguistic accuracy, cultural appropriateness, and consistency across all languages.

1.4.2.7.2. Testing Approach

The contractor shall adopt a phased and iterative testing process, including:

- Internal release: The initial internal version of the chatbots shall be released for testing by Commission experts and native-language testers.
- Feedback after two weeks: Feedback from internal testers shall be collected after a two-week period and integrated into system improvements.
- Public release after six weeks: A wider release, including user testing with the intended target audience (e.g. citizens, SMEs), shall follow approximately six weeks after the internal release.

1.4.2.7.3. Performance and Accuracy Tracking

The contractor shall:

- Prepare a Performance Matrix clearly outlining precision rates, response times, language-specific accuracy, and system stability indicators.
- Document the testing methodology, datasets, precision measurements, user feedback, and system refinements in the final reporting package.

1.4.2.8. Continuous Quality Monitoring

The contractor must implement mechanisms to monitor and maintain accuracy over time, including updates to the knowledge base, retraining of the chatbot where necessary, and regular accuracy assessments.

The contractor shall propose solutions for ongoing quality assurance beyond the contract period, ensuring that the chatbot remains reliable, accurate, and up-to-date as the regulatory frameworks evolve.

1.4.2.9. Post-Launch Support and Monitoring

The contractor shall provide post-launch support and monitoring services to ensure the chatbot remains fully functional, accurate, and secure after deployment.

The post-launch support must include, at a minimum:

- Operational Monitoring: Continuous monitoring of system availability, response times, and error rates to ensure the chatbot performs reliably under real-world usage. The contractor must provide mechanisms for the detection and prompt resolution of technical issues.
- Incident Management: The contractor must define and implement an incident management procedure, including a clear response time commitment for resolving critical issues, security incidents, and service disruptions.
- Multilingual Performance Monitoring: Ongoing tracking of chatbot performance across supported languages. The contractor must address any emerging accuracy or linguistic issues, including errors reported by users or detected through analytics.
- Support Availability: The contractor must offer a support service (e.g. helpdesk or ticketing system) with clearly defined availability (e.g. working hours, response times) throughout the post-launch phase.
- Handover and Knowledge Transfer: Before the end of the contract period, the contractor shall provide full documentation package (see 1.4.3.6 Documentation Package), training if necessary, and a knowledge transfer session to ensure that the European Commission or its designated contractors can take over system maintenance and monitoring.

1.4.3. Deliverables

The contractor shall deliver two fully functional chatbots. The delivery shall include all necessary documentation, tools, and technical components required for initial deployment, evaluation, and operational continuity.

The deliverables listed below must be provided by the contractor:

1.4.3.1. Planning Document

A detailed work plan should specify the management structure as well as the responsibility of each member of the team. This work plan should include a list of tasks to be performed, with clear and realistic phases and milestones. Resources should be clearly associated to each task, i.e. for example the estimate number of man days for each task or phase, etc.

1.4.3.2. Technical Architecture and Design Document

A comprehensive document describing, notably, the IT system structure, infrastructure, deployment setup, cybersecurity measures, integrations, and the use of standard and open-source technologies.

This document shall focus exclusively on the technical architecture and system-level components, including access control mechanisms, monitoring tools, and system integrations. It shall not cover the chatbot's conversational logic, user guidance flows, or knowledge base content, which are addressed under the Documentation Package (section 1.4.3.6).

The document must include a Data Flow Diagram (DFD) that clearly illustrates the flow of data between system components, infrastructure layers, and IT processes. This includes any interactions between front-end interfaces, backend services, vector databases, identity systems, and monitoring tools (e.g. EU Login, SIEM, cloud infrastructure, etc.).

During the whole contract period, the document must be updated regularly, and whenever there are major changes to the system architecture or security model. Updated versions must be submitted to DG CNECT for review and validation. The contractor shall liaise with the designated security contact point in DG CNECT to ensure that all relevant security aspects are covered appropriately. DG CNECT reserves the right to review and request revisions to ensure alignment with Commission standards and evolving cybersecurity practices.

1.4.3.3. Pre-development Readiness Checklist

A validated internal checklist confirming that the development environment, tools, access credentials, and key workflows are in place. A basic chatbot mock-up may be included at this stage.

1.4.3.4. Chatbots

Two operational, web-accessible chatbot applications, each implemented, configured and deployed in line with the functional and technical specifications set out in Section 1.4.2.4. This includes the configured chatbot instances, their underlying configuration and prompt logic, integration with the agreed data sources, deployment within the Commission infrastructure, and the associated technical and user documentation necessary for operation, maintenance and further development.

1.4.3.5. Analytics Dashboard

A web-based reporting interface providing aggregated insights into chatbots usage, including metrics such as number of queries, most frequently addressed topics, user drop-off points, and recurring user behaviour patterns or misunderstandings, in line with the reporting and interface requirements set out in section 1.4.2.4.

1.4.3.6. Documentation Package

A complete documentation package shall be delivered, focusing on the chatbot's functional logic, content, and data protection aspects. This package shall include:

- Documentation of the knowledge base supporting the chatbot, including legal and policy sources such as the DSA, the AI Act, etc. including a list of the sources of the content fed into the chatbot, with an indication of the respective copyright status and EU ownership or licence rights, i.e., (a) copyright-free/public domain; (b) copyright owned by the EU; or (c) licensed to the EU, with details regarding the specific licence.
- Data protection documentation (see 1.4.2.5.), namely a Data Protection Risk Assessment, which includes, among others, i) a detailed description of how the chatbot guides users based on input categories, conversation flows, and use cases, ii) a mapping of all potential personal data processing activities, iii) an explanation of how data protection principles will be applied

(e.g. lawfulness — including legal basis and necessity/proportionality — purpose limitation, data minimisation, accuracy, storage, processing location, and retention). The contractor shall also detail who has access to raw and processed data at each stage of the data pipeline (collection, anonymisation, processing), and provide a log of access rights. Only the European Commission or specifically authorised entities may retain or access raw or anonymised data post-deployment. This DPRA also includes an assessment of the need for a Data Protection Impact Assessment (DPIA) in line with Article 39 EUDPR. If a DPIA is necessary, the contractor will draft it under the supervision of the Commission.

As mentioned above, the contractor shall support the Commission with the preparation of other data protection documentation, namely the data protection record and privacy statement.

This Package shall not duplicate content from section 1.4.3.2 (IT infrastructure, system security, or deployment design).

The contractor must progressively develop this documentation throughout the entire post-launch phase. A consolidated and finalised version shall be included in the final reporting and handover deliverables at the end of the contract period.

1.4.3.7. Risk Assessment

The contractor shall prepare and deliver a comprehensive report describing how the contractor has identified, assessed, and addressed the key risks associated with the design, deployment, and maintenance of the public-facing chatbots.

The report shall:

- Describe the risk identification process followed by the contractor.
- Explain how the risks were assessed across different impact dimensions.
- Provide the mitigation measures the contractor has put in place or plans to implement.

The report must specifically explain how the following risk areas have been considered and addressed:

- ***Reputational Risks***

The contractor shall describe how the risks related to inaccurate, misleading, or linguistically incorrect responses have been identified and addressed. This should include the accuracy validation methods, multilingual testing strategies, and quality monitoring processes that have been put in place to protect the European Commission's credibility and user trust.

- ***Vendor Lock-in Risks***

The contractor shall explain how the risk of vendor lock-in has been assessed and mitigated. The report must describe how the solution has been designed to remain model-agnostic and adaptable to future providers, open-source large language models (LLMs), or new technological environments.

- ***Multilingual Performance Risks***

The contractor shall describe how the risks related to degraded chatbot performance in smaller languages or languages with limited LLM support have been identified and addressed. The report must include details of specific validation processes and mitigation measures implemented for these languages.

❖ ***Security and Operational Risks***

The contractor shall explain how security and operational risks, such as cyberattacks, data breaches, system failures, and maintenance challenges, have been identified and mitigated. The report shall demonstrate alignment with EU cybersecurity frameworks and the Commission's security protocols.

IT Security Workshops

In addition, the contractor shall actively participate in two dedicated IT security workshops organised by the Commission services. The aim of these workshops is to support the preparation of the IT Security Plan required before the public go-live of the chatbots. The contractor is expected to contribute substantively, both through written input and by presenting and discussing their proposed mitigation measures during the sessions.

1.4.3.8. Final Reporting and Handover Package

By Month 5, the contractor shall submit a Final Reporting and Handover Package consolidating the key outputs of the development and deployment phase, including final documentation, deployment details, and handover materials. This deliverable shall confirm that the chatbot applications are fully deployed and ready for public operation.

1.4.3.9. Interim and Final Post-Launch Reports

An Interim Post-Launch Report shall be submitted in Month 12. The report shall briefly describe the operational status of the chatbot applications, including availability, incidents addressed, corrective or adaptive maintenance performed, and minor improvements implemented during the post-launch phase (1.4.4.). Its acceptance by the Commission services shall constitute an interim post-launch deliverable linked to the interim payment.

In Month 18, at the end of the post-launch phase, the contractor shall submit a Final Post-Launch Report, summarising the activities performed, issues addressed, improvements implemented, and the overall status of the solution. The report shall be subject to formal approval by the Commission services and shall constitute the final deliverable linked to the final payment under the contract.

1.4.4. Post-Launch Phase

The post-launch phase shall cover a minimum period of 13 months following the public release of the chatbot applications. During this phase, the contractor shall:

- Ensure the chatbot remains fully operational.
- Provide timely support through the agreed support service (e.g. helpdesk or ticketing system).
- Address any unforeseen issues, bugs, or performance adjustments identified after deployment.
- Integrate minor improvements based on user feedback.

The post-launch phase is intended to stabilise the solution and ensure smooth adoption by end-users.

The contractor must provide a support service to ensure timely assistance throughout the post-launch phase.

The support service shall include:

- A helpdesk or ticketing system allowing the European Commission to report issues, request clarifications, or submit feedback.

- Clearly defined availability periods, including:
    - Standard working hours (e.g. Monday to Friday, 09:00 to 17:00 CET).
    - A maximum initial response time of two working days for non-critical issues.
    - A faster response time for critical issues.

The contractor must provide:

- A single point of contact for support requests.
- A mechanism to track and follow up on the status of each ticket.
- Periodic updates on issue resolution progress.

The support service must cover the entire post-launch phase and shall ensure that any critical operational issue impacting chatbot functionality is addressed without delay to minimise user disruption.

1.4.5. Meetings

A schedule of meetings will be agreed with the contractor for this assignment. Such meetings will be attended by representatives of the European Commission, the project manager leader and other members of the contractor's team, as required. The meetings will be chaired by a Commission representative and will take place in Brussels or online, subject to agreement by the European Commission.

The aim of the meetings will be to guide the work of the contractor. They will allow setting-up the initial orientations, review progress in critical milestones and review the deliverables of the assignment.

Meetings are expected to be organised at least at key stages of the assignment, in particular during the initial project initiation and planning phase (Month 1), in connection with the validation of the technical proposal and the technical architecture and design, around the internal release and testing of the chatbot applications (Month 3), in relation to the public deployment (Month 4), and in the context of the final reporting and handover (Month 5), without prejudice to the organisation of additional meetings whenever required. In addition, a dedicated meeting shall be organised at the end of the post-launch phase to formally conclude the post-launch phase.

Within three days following each meeting, the contractor will circulate minutes of the meeting to all participants, together with copies of presentations made during the meeting or other related documents. The minutes shall be concise and concentrate on major decisions and shall list the open action points for the next reporting period.

1.4.5.1 Inception and validation meetings

As part of the inception phase, the contractor shall deliver a consolidated work plan, building upon the initial technical proposal submitted during the tendering process. This deliverable shall be informed by an Inception Meeting with representatives of the European Commission, during which the overall scope, work breakdown structure, timeline, key milestones, and roles and responsibilities shall be discussed and validated.

The inception phase shall be concluded by a dedicated Validation Meeting with the Commission services, during which the consolidated work plan and the updated technical proposal shall be formally validated, confirming that all elements are aligned with the Commission's expectations and ready for implementation.

1.4.5.2. Monthly Progress Meetings

The contractor shall organise monthly progress meetings with the contracting authority to monitor the overall status of implementation. These meetings shall serve to review deliverables, track progress against planned milestones, and validate interim outputs.

They will also provide a forum to identify emerging risks or challenges, propose mitigation measures, and, where necessary, adjust the implementation plan in agreement with the contracting authority. The contractor shall provide concise minutes after each meeting to document decisions and action points, ensuring transparency and follow-up.

1.4.5.3. Handover Session

At the end of the contract, the contractor shall organise a Final Handover Meeting with the contracting authority to formally close the project and ensure a smooth transition beyond the contract period. This meeting shall serve to present and validate all final deliverables, including documentation, technical components, and the complete handover package. It will also provide an opportunity to transfer operational knowledge, explain maintenance procedures, and address any outstanding technical or operational questions from the contracting authority.

1.4.5.4. Bi-Monthly Post-Launch Progress Meetings

During the post-launch phase, the contractor shall organise bi-monthly progress meetings with the contracting authority to monitor the operational status of the solution. These meetings shall serve to review post-launch activities, assess system stability and performance, and follow up on support actions and minor improvements.

The meetings shall also provide a forum to identify emerging issues or risks, agree on corrective measures where necessary, and ensure continued alignment with the contracting authority. The contractor shall provide concise minutes after each meeting to document discussions, decisions, and action points, ensuring transparency and effective follow-up.

1.4.5.5. End of Post-Launch Phase Meeting

At the end of the contract, the contractor shall organise an End of Post-Launch Phase Meeting with the contracting authority to formally close the project. This meeting shall serve to present and validate the final deliverables, including the Final Post-Launch Report. It shall also ensure the effective transfer of operational knowledge, including maintenance procedures and support arrangements, and provide an opportunity to address any outstanding technical or operational questions from the contracting authority.

1.4.6. Timetable

The contractor shall follow the timeline below. The timetable specifies the sequence of key activities, deliverables, and their respective deadlines, expressed in project months starting from the date of contract signature.

Title	Type	Due month (at the latest)	Linked to payment
Inception and validation Meeting (1.4.5.1)	Meeting	Month 1	No

Title	Type	Due month (at the latest)	Linked to payment
Validation of the technical specifications (1.4.5.1)	Meeting	Month 1	No
Planning Document (1.4.3.1)	Deliverable (Document)	Month 1	No
Technical Architecture and Design Document (1.4.3.2)	Deliverable (Document)	Month 1	No
Pre-development Readiness Checklist (1.4.3.3)	Deliverable (Document)	Month 1	No
Monthly Progress Meeting (1.4.5.2)	Meeting	Month 1	No
Monthly Progress Meeting (1.4.5.2)	Meeting	Month 2	No
Web-Accessible Chatbots (Internal Release) (1.4.3.4)	Deliverable (System)	Month 3	No
Analytics Dashboard (1.4.3.5)	Deliverable (System)	Month 3	No
Documentation Package (1.4.3.6)	Deliverable (Document)	Month 3	No
Risk Assessment Report (1.4.3.7)	Deliverable (Document)	Month 3	No
Monthly Progress Meeting (1.4.5.2)	Meeting	Month 3	No
Monthly Progress Meeting (1.4.5.2)	Meeting	Month 4	No
Public Release of the Two Chatbots	Deliverable (System)	Month 5	No
Handover Session (1.4.5.3)	Meeting	Month 5	No
Final Reporting and Handover Package (1.4.3.8)	Deliverable (Document)	Month 5	Yes
Bi-Monthly Post-Launch Progress Meetings (1.4.5.4)	Meeting	Month 7	No
Bi-Monthly Post-Launch Progress Meetings (1.4.5.4)	Meeting	Month 9	No
Bi-Monthly Post-Launch Progress Meetings (1.4.5.4)	Meeting	Month 11	No
Interim Post-Launch Report (1.4.3.9)	Deliverable (Document)	Month 12	Yes
Bi-Monthly Post-Launch Progress Meetings (1.4.5.4)	Meeting	Month 13	No
Bi-Monthly Post-Launch Progress Meetings (1.4.5.4)	Meeting	Month 15	No
Bi-Monthly Post-Launch Progress Meetings (1.4.5.4)	Meeting	Month 17	No
End of Post-Launch Phase Meeting (1.4.5.5)	Meeting	Month18	No
Final Post-Launch Report (1.4.3.9.)	Deliverable (Document)	Month 18	Yes

1.4.7. Terms of approval of reports and deliverables

For the deliverables listed under Section 1.4.3, the following approval process shall apply:

1.4.7.1. Reports and Documentation

Upon submission of each report or document, the Commission shall have 30 calendar days to:

- Approve the deliverable,
- Or reject it and request a revised version.

If no feedback is provided within this period, the deliverable shall be deemed approved. In case of rejection, the contractor shall submit a revised version within 15 calendar days of receiving the Commission's comments. The revised version shall then be subject to the same 30-day review period.

1.4.7.2. Technical Components and Tools

For deliverables involving deployed systems or technical tools (e.g., the chatbots prototype, analytics dashboards, etc.), the Commission shall have 30 calendar days from receipt to evaluate and:

- Approve the deliverable,
- Or reject it and request further development, refinement, or correction.

The contractor shall have 15 calendar days to submit a revised version in case of rejection. The revised deliverable shall then follow the same 30-day evaluation timeline.

1.4.8. Report format of the deliverables

All reports must be written in English. They should be consistent in style (headings, margins, citations, bibliography, etc.) and contain a short executive summary. The contractor is required to properly apply quotation techniques and particular care will be taken to verify improper re-use of existing material.

All reports will be submitted in electronic format (.doc, .xls, .ppt or equivalents in open formats) and in a .pdf format suitable for publication by the Commission's services on Commission websites. Exchange of advance copies as well as other non-formal communications shall take place via electronic mail.

1.5. Place of performance: where will the contract be performed?

The services will be performed at the following locations:

- the contractor's premises
- the premises of DG CNECT (European Commission, Brussels) where coordination meetings, presentations, or reviews may take place.

1.6. Nature of the contract: how will the contract be implemented?

The procedure will result in the conclusion of a direct contract.

In direct contracts all the terms governing the provision of the services, supplies or works are defined at the outset. Once signed, they can be implemented directly without any further contract procedures.

Tenderers need to take full account of the full set of procurement documents, including the provisions of the draft contract as the latter will define and govern the contractual relationship to be established between the contracting authority and the successful tenderer. Special attention is to be paid to the provisions specifying the rights and obligations of the contractor, in particular those on payments, performance of the contract, confidentiality, and checks and audits.

☝ Please be aware that if a tenderer to whom the contract is awarded (any of the group members in case of a joint tender) has established debt(s) owed to the Union, the European Atomic Energy Community or an executive agency when the latter implements the Union budget, such debt(s) may

be offset, in line with Articles 101(1) and 102 of the Financial Regulation[1] and the conditions set out in the draft contract, against any payment due under the contract. The contracting authority will verify the existence of overdue debts of the successful tenderer (any of the group members in case of a joint tender), and, if any such debt is found, will inform the tenderer (the group leader in case of a joint tender who will then have the obligation to inform all other group members before signing the contract) that the debt(s) may be offset against any payment under due the contract.

1.7. Volume and value of the contract: how much do we plan to buy?

The maximum total amount of all purchases under this call for tenders is indicated under Section 2.1.3 of the contract notice. The volumes/values of the purchases over the total duration of the contract are specified in Section 1.4 of these specifications.

Within three years following the signature of the contract resulting from the current call for tenders, the contracting authority may use the negotiated procedure under point 11.1.e of Annex 1 to the Financial Regulation to procure new services from the contractor up to a maximum 50% of the initial contract value. These services would consist in the repetition of similar services entrusted to the contractor and would be awarded under the same conditions.

1.8. Duration of the contract: how long do we plan to use the contract?

The contract resulting from the award of this call for tenders will be concluded for at most 18 months. The details of the initial contract duration and possible renewals are set out in the draft contract.

1.9. Electronic exchange system: can exchanges under the contract be automated?

For all exchanges with the contractor during the implementation of the contract as well as for future possible subsequent proceedings, including, but not limited to, for the purposes of EDES (European Union's Early Detection and Exclusion System), the contracting authority may use an electronic exchange system meeting the requirements of Article 151 of the Financial Regulation. At the request of the contracting authority, the use of such a system shall become mandatory for the contractor at no additional cost for the contracting authority. Details on specifications, access, terms and conditions of use will be provided in advance.

1.11. Other provisions

1.11.1. Fraud prevention and detection

The contractor must assist the contracting authority in its efforts on fraud prevention and detection.

The contractor undertakes to impose the fraud prevention obligations upon its subcontractors and personnel in the relevant contracts signed with them. Upon request, the contractor must provide evidence to the contracting authority that those obligations have been included in the relevant agreements with its subcontractors and personnel.

[1] Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council of 23 September 2024 on the financial rules applicable to the general budget of the Union (recast) (OJ L, 2024/2509, 26.09.2024, ELI: http://data.europa.eu/eli/reg/2024/2509/oj)

1.11.2. Environmental considerations

Environmental considerations shall be taken into account by the contractor throughout the complete life cycle of providing products or services in the implementation of the contract.

When applicable, the contractor shall assist the Commission to perform its commitments as set in the EMAS EC Environmental Policy[3] and shall follow EMAS best practices.

1.11.3. Equal opportunities

The contractor shall observe a policy on the promotion of equality and diversity in the implementation of the contract, by applying the principles of non-discrimination and equality set out in the EU Treaties in full and in their entirety.

In the implementation of the contract, the contractor shall establish, maintain and promote an open and inclusive working environment which respects human dignity and the principles of equal opportunities, especially through the removal of all obstacles to recruitment and all potential discrimination based on sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation.

[3] Available at 2022_12_13_Environmental_Policy_2022_adopted_by_the_ESC_on_4_October_EN.pdf (europa.eu)

2. GENERAL INFORMATION ON TENDERING

2.1. Legal basis: what are the rules?

This call for tenders is governed by the provisions of the Financial Regulation.

The contracting authority has chosen to award the contract resulting from this call for tenders through an open procedure pursuant to Article 167(1)(a) of the Financial Regulation.

In this procedure any interested economic operator (any natural or legal person who offers to supply products, provide services or execute works) may submit a tender.

2.2. Entities subject to restrictive measures and rules on access to procurement: who may submit a tender?

Tenderers must ensure that no involved entities (see Section 2.4) nor any subcontractors, including those which do not need to be identified in the tender (see Section 2.4.2), are subject to EU restrictive measures adopted under Article 29 of the Treaty on the European Union (TEU) or Article 215 of the Treaty on the Functioning of the EU (TFEU)[4], consisting of a prohibition to make available or transfer funds or economic resources or to provide financing or financial assistance to them directly or indirectly, or of an asset freeze. The prohibition applies throughout the whole performance of the contract.

Participation in this call for tenders is open on equal terms to all natural and legal persons coming within the scope of the Treaties, as well as to international organisations.

It is also open to all natural and legal persons established in a third country provided that it has a special agreement with the European Union in the field of public procurement on the conditions laid down in that agreement.

As the Agreement on Government Procurement[5] concluded within the World Trade Organisation applies, the participation to this call for tenders is also open to all natural and legal persons established in the countries that have ratified this Agreement, on the conditions laid down therein.

The rules on access to procurement do not apply to entities on whose capacity tenderers rely to fulfil the selection criteria nor to subcontractors. Subcontracting may not be used with the intent or effect to circumvent the rules on access to procurement.

To enable the contracting authority to verify the access, each tenderer must indicate its country of establishment (in case of a joint tender – the country of establishment of each group member) and must present the supporting evidence normally acceptable under the law of that country. The same document(s) could be used to prove country/-ies of establishment and the delegation(s) of the authorisation to sign, as described in Section 4.3.

2.3. Registration in the Participant Register: why register?

Any economic operator willing to participate in this call for tenders must be registered in the

[4] Please note that the EU Official Journal contains the official list and, in case of conflict, its content prevails over that of the EU Sanctions Map.

[5] https://www.wto.org/english/tratop_E/gproc_e/gp_gpa_e.htm

Participant Register - an online register of organisations and natural persons (participants) participating in calls for tenders or proposals of the European Commission and other EU institutions/bodies.

On registering each participant obtains a Participant Identification Code (PIC, 9-digit number), which acts as its unique identifier in the Participant Register. A participant needs to register only once – the information provided can be further updated or re-used by the participant in other calls for tenders or calls for proposals of the European Commission and other EU institutions/bodies.

☝ **Each participant needs to ensure that its SME status in the Participant Register is registered and kept up to date.**

At any moment during the procurement procedure, the Research Executive Agency Validation Services (hereafter *the EU Validation Services*) may contact the participant and ask for supporting documents on legal existence and status and financial capacity. The requests will be made through the register's messaging system to the e-mail address of the participant's contact person indicated in the register. It is the responsibility of the participant to provide a valid e-mail address and to check it regularly. The documents that may be requested by *the EU Validation Services* are listed in the EU Grants and Tenders Rules on Legal Entity Validation, LEAR appointment and Financial Capacity assessment.

☝ **Please note that a request for supporting documents by the *EU Validation Services* in no way implies that the tenderer has been successful.**

2.4. Ways to submit a tender: how can economic operators organise themselves to submit a tender?

Economic operators can submit a tender, either as a sole economic operator (sole tenderer) or as a group of economic operators (joint tender)[6]. In either case subcontracting is permitted.

Tenders must be drawn and submitted in complete independence and autonomously from the other tenders. A declaration in this regard by each tenderer (in case of a joint tender, by the group leader) shall be requested ***(Annex 2)***.

A natural or legal person cannot participate at the same time and within the same procedure either as member of two or more groups of economic operators or as a sole tenderer and member of another group of economic operators. In such case, all tenders in which that person has participated, either as sole tenderer or as member of a group of economic operators, will be rejected.

Economic operators linked by a relationship of control or of association (e.g. belonging to the same economic/corporate group) are allowed to submit different and separate tenders, provided that each tenderer is able to demonstrate that its tender was drawn independently and autonomously.

A natural or legal person may act as subcontractor for several tenderers as long as the tenders are drawn and submitted in complete independence and autonomously from each other. However, cross subcontracting among tenderers is forbidden, more precisely an entity "A" may participate as tenderer (either as sole tenderer or as member of a group of economic operators) and as subcontractor to another tenderer "B" within the same procurement procedure. However, in this case it is forbidden that tenderer "B" (or any of its participating members in case of a group of economic operators) is at

[6] Each economic operator participating in the joint tender is referred to as "group member".

the same time subcontractor for tenderer "A" (or for the group of economic operators in which "A" participates) within the same procurement procedure. In this case, both tenders A and B shall be rejected.

In order to fulfil the selection criteria set out in Section 3.2 the tenderer can rely on the capacities of subcontractors (see Section 2.4.2) or other entities that are not subcontractors (see Section 2.4.3).

An **"involved entity"** is any economic operator involved in the tender. This includes the following four categories of economic operators:

- sole tenderer,
- group members (including group leader),
- identified subcontractors (see Section 2.4.2), and
- other entities (that are not subcontractors) on whose capacity the tenderer relies to fulfil the selection criteria.

The role of each entity involved in a tender must be clearly specified in the eSubmission application: i) sole tenderer, ii) group leader (in case of a joint tender), iii) group member (in case of a joint tender), or iv) subcontractor[7].

For an entity on whose capacities the tenderer relies to fulfil the selection criteria (that is not a subcontractor), this role is defined in the commitment letter (***Annex 5.2***)

2.4.1. Joint tenders

A joint tender is a situation where a tender is submitted by a group (with or without legal form) of economic operators regardless of the link they have between them in the group. The group as a whole is considered a tenderer[8].

All group members assume joint and several liability towards the contracting authority for the performance of the contract as a whole.

Group members must appoint from among themselves a group leader (the group leader) as a single point of contact authorised to act on their behalf in connection with the submission of the tender and all relevant questions, clarification requests, notifications, etc., that may be received during the evaluation, award and until the contract signature. All group members (including the group leader) must sign an Agreement/Power of attorney drawn up in the model attached in **Annex 3**.

The joint tender must clearly indicate the role and tasks of each group member, including those of the group leader who will act as the contracting authority's contact point for the contract's administrative or financial aspects and operational management. The group leader will have full authority to bind the group and each of its members during contract execution.

If the joint tender is successful, the contracting authority shall sign the contract with the group leader, authorised by the other members to sign the contract also on their behalf via the Agreement/Power of attorney drawn up in the model attached in ***Annex 3***.

Changes in the composition of the group during the procurement procedure (after the deadline for

[7] Only identified subcontractors (see Section 2.4.2) must be specified in the eSubmission application.

[8] References to *tenderer* or *tenderers* in this document shall be understood as covering both sole tenderers and groups of economic operators submitting a joint tender.

submission of tenders and before contract signature) shall lead to rejection of the tender, with the exception of the following cases:

- case of a merger or takeover of a group member (universal succession), provided that the following cumulative conditions are fulfilled:

  - the new entity is not subject to restrictive measures, has access to procurement (see Section 2.2) and is not in an exclusion situation (see Section 3.1),
  - all the tasks assigned to the former entity are taken over by the new entity member of the group,
  - the group meets the selection criteria (see Section 3.2),
  - the change must not make the tender non-compliant with the procurement documents,
  - the terms of the originally submitted tender are not altered substantially and the evaluation of award criteria of the originally submitted tender are not modified,
  - the new entity undertakes to replace the former entity for the implementation of the contract, in case of an award.

- case where a group member is subject to restrictive measures or does not have access to procurement (see Section 2.2) or is in an exclusion situation (see Section 3.1), provided the following cumulative conditions are fulfilled:

  - none of the remaining group members is subject to restrictive measures (see Section 2.2),
  - all the remaining group members have access to procurement (see Section 2.2),
  - the remaining group members meet the selection criteria (see Section 3.2),
  - the change must not make the tender non-compliant with the procurement documents,
  - the terms of the originally submitted tender are not altered substantially and the evaluation of award criteria of the originally submitted tender are not modified,
  - the continuation of the participation of the remaining group members in the procurement procedure does not put the other tenderers in a competitive disadvantage,
  - the remaining group members undertake to implement the contract, in case of an award, without the excluded group member.

The replacement of the group member not having access to procurement or in a situation of exclusion is not allowed.

2.4.2. Subcontracting

Subcontracting is the situation where the contractor enters into legal commitments with other economic operators, which will perform part of the contract on its behalf. The contractor retains full liability towards the contracting authority for performance of the contract as a whole.

The following shall not be considered subcontracting:

a) Use of workers posted to the contractor by another company owned by the same group and established in a Member State ("intra-group posting" as defined by Article 1, 3, (b) of Directive 96/71/EC concerning the posting of workers in the framework of the provision of services).
b) Use of workers hired out to the contractor by a temporary employment undertaking or placement agency established in a Member State ("hiring out of workers" as defined by Article 1, 3, (c) of Directive 96/71/EC concerning the posting of workers in the framework of the provision of services).
c) Use of workers temporarily transferred to the contractor from an undertaking established outside the territory of a Member State and that belongs to the same group ("intra-corporate

transfer" as defined by Article 3, (b) of Directive 2014/66/EU on the conditions of entry and residence of third-country nationals in the framework of an intra-corporate transfer).

d) Use of staff without employment contract ("self-employed persons working for the contractor"), without the tasks of the self-employed persons being particular well-defined parts of the contract.
e) Use of suppliers and/or transporters by the contractor, in order to perform the contract at the place of performance, unless the economic activities of the suppliers and/or the transporting services are within the subject of this call for tenders (see Section 1.4).
f) Performance of part of the contract by members of an EEIG (European Economic Interest Grouping), when the EEIG is itself a contractor or a group member.

The persons mentioned in points a), b), c) and d) above will be considered as "personnel" of the contractor as defined in the contract.

All contractual tasks may be subcontracted unless the procurement documents expressly reserve the execution of certain critical tasks to the sole tenderer itself, or in case of a joint tender, to a group member.

By filling in the form available in ***Annex 4*** (List of identified subcontractors), tenderers are required to give an indication of the proportion of the contract that they intend to subcontract, as well as to identify and describe briefly the envisaged contractual roles/tasks of subcontractors meeting any of these conditions (hereafter referred to as *identified subcontractors*):

- subcontractors on whose capacities the tenderer relies upon to fulfil the selection criteria as described under Section 3.2;
- subcontractors whose intended individual share of the contract, known at the time of submission, is above 15%.

Any such subcontractor must provide the tenderer with a commitment letter drawn up in the model attached in ***Annex 5.1*** and signed by its authorised representative.

☝ Each tenderer shall identify such subcontractors and provide the commitment letters with its tender. The information must be true and correct at the time of submitting the tender. Any changes or additions regarding the envisaged subcontractors after the deadline for submission of tenders must be justified to the contracting authority.

The above rules apply also where the economic operators, which will perform part of the contract on behalf of a successful tenderer, belong to the same economic/corporate group as the sole tenderer or a member of the group submitting the joint tender.

Changes concerning subcontractors identified in the tender (withdrawal/replacement of a subcontractor, additional subcontracting) during the procurement procedure (after the deadline for submission of tenders and before contract signature) require the prior written approval of the contracting authority subject to the following verifications:

- any new subcontractor is not subject to restrictive measures, has access to procurement if the rules on access to procurement apply also to subcontractors (see Section 2.2) and is not in an exclusion situation (see Section 3.1),
- the tenderer still fulfils the selection criteria and the new subcontractor fulfils the selection criteria applicable to it individually, if any;
- the terms of the originally submitted tender are not substantially altered, i.e. all the tasks assigned to the former subcontractor are taken over by another involved entity, the change

does not make the tender non-compliant with the tender specifications, and the evaluation of the award criteria of the originally submitted tender is not modified.

Subcontracting to subcontractors identified in a tender that was accepted by the contracting authority and resulted in a signed contract, is considered authorised.

2.4.3. Entities (not subcontractors) on whose capacities the tenderer relies to fulfil the selection criteria

In order to fulfil the selection criteria a tenderer may also rely on the capacities of other entities (that are not subcontractors), regardless of the legal nature of the links it has with them. It must in that case prove that it will have at its disposal the resources necessary for the performance of the contract by producing a commitment letter in the model attached in ***Annex 5.2***, signed by the authorised representative of such an entity, and the supporting evidence that those other entities have the respective resources[9].

☝ The above rules apply also where the economic operators on whose capacities the tenderer relies to fulfil the selection criteria (that are not subcontractors) belong to the same economic/corporate group as the sole tenderer or a member of the group submitting the joint tender.

2.4.4. Rules common to subcontractors and entities (not subcontractors) on whose capacities the tenderer relies to fulfil the selection criteria

If a successful tenderer intends to rely on another entity to meet the minimum levels of economic and financial capacity, the contracting authority may require the entity to sign the contract or, alternatively, to provide a joint and several first-call financial guarantee for the performance of the contract.

With regard to technical and professional selection criteria, a tenderer may rely on the capacities of other entities only when these entities will perform the works or services for which these particular capacities are required. In such cases, they will either assume the role of subcontractors, or, where the exceptions listed in Section 2.4.2 are appliable, they will assume the role of entities on whose capacities the tenderer relies to fulfil the selection criteria without being subcontractors.

☝ Relying on the capacities of other entities is only necessary when the capacity of the tenderer is not sufficient to fulfil the required minimum levels of capacity. Abstract commitments that other entities will put resources at the disposal of the tenderer will be disregarded.

[9] This does not apply to subcontractors on whose capacity the tenderer relies to fulfil the selection criteria – for these the documentation required for subcontractors must be provided.

3. EVALUATION AND AWARD

The evaluation of the tenders that comply with the submission conditions will consist of the following elements:

- Check if the tenderer has access to procurement (see Section 2.2);
- Verification of administrative compliance (if the tender is drawn up in one of the official EU languages and the required documents signed by duly authorised representative(s) of the tenderer);
- Verification of non-exclusion of tenderers on the basis of the exclusion criteria;
- Selection of tenderers on the basis of selection criteria;
- Evaluation of tenders: compliance with the requirements of the procurement documents and on the basis of the award criteria.
- Verification if the tenderer including any subcontractor is not subject to EU restrictive measures (see Section 2.2) or any other rejection grounds from the award procedure.

The contracting authority will evaluate the above mentioned elements in the order that it considers to be the most appropriate.

If the evaluation of one or more elements demonstrates that there are grounds for rejection, the tender will be rejected and will not be subjected to full evaluation. The rejected tenderers will be informed of the ground for rejection without being given any feedback on the non-assessed content of their tenders. The ranked tenderers will have access to information on the relative advantages of the successful tenderer(s) and its (their) total financial offer amount, if they request so in writing after being informed of the result of the procedure. This will be without the prejudice to further checks and to the provision of supporting documents on exclusion and/or selection criteria if the contract cannot be signed with the presumed winner(s). Only the tenderer for whom the verification of all elements did not reveal grounds for rejection can be awarded the contract resulting from this call for tenders.

The evaluation will be based on the information and evidence contained in the tenders and, if applicable, on additional information and evidence provided at the request of the contracting authority during the procedure. If any of the declarations or information provided proves to be false, the contracting authority may impose administrative sanctions (exclusion or financial penalties) on the entity providing the false declarations/information.

For the purposes of the evaluation related to exclusion and selection criteria the contracting authority may also refer to publicly available information, in particular evidence that it can access on a national database free of charge.

3.1. Exclusion criteria

The objective of the exclusion criteria is to assess whether the tenderer is in any of the exclusion situations listed in Article 138(1) of the Financial Regulation.

Tenderers found to be in an exclusion situation will be rejected.

As evidence of non-exclusion, each tenderer[10] needs to submit with its tender a Declaration on

[10] See Annex 1 which of the involved entities participating in a tender need to provide the Declaration on Honour.

Honour[11] in the model available in ***Annex 2***.[12] The declaration must be signed by an authorised representative of the entity providing the declaration. Where the declaration has been signed by hand, the original does not need to be submitted to the contracting authority, but the latter reserves the right to request it from the tenderer at any time during the record-keeping period specified in Section 4.3.

The initial verification of non-exclusion of tenderers will be done on the basis of the submitted declarations and consultation of the European Union's Early Detection and Exclusion System.

Evidence will be requested only from the presumed successful tenderer before the award decision, without prejudice to the possibility for the contracting authority to ask any tenderer at any moment during the procedure[14] to submit an updated declaration or all or part of the supporting documents where this is necessary to ensure the proper conduct of the procedure.

The Contracting authority may also request information on natural or legal persons that are members of the administrative, management or supervisory body or that have powers of representation, decision or control, including legal and natural persons within the ownership and control structure and beneficial owners, and appropriate evidence that none of those persons are in one of the exclusion situations referred to in Section A point (1) (c) to (f) of the Declaration on Honour.

All tenderers are **invited to prepare in advance the documentary evidence**, since they may be requested to provide such evidence within a short deadline.

☝ If the tenderer does not provide valid documentary evidence within the deadlines set by the contracting authority, the latter reserves the right to reject the tender. In any event, in case a tenderer proposed for the award of the contract fails to comply with the above evidence requirement, its tender will be rejected, unless the tenderer can justify the failure on the grounds of material impossibility to provide such evidence.

Annex 1 specifies which of the involved entities participating in a tender need to provide the Declaration on Honour and, when requested by the contracting authority, the supporting evidence.

Please note that a request for evidence in no way implies that the tenderer has been successful.

3.2. Selection criteria

The objective of the selection criteria is to assess whether the tenderer has the legal, regulatory, economic, financial, technical and professional capacity to perform the contract.

The selection criteria for this call for tenders, including the minimum levels of capacity, the basis for

[11] The European Single Procurement Document (ESPD) may not be used yet in calls for tenders of the European Commission.

[12] Unless the same declaration has already been submitted for the purposes of another award procedure of the European Commission, the situation has not changed, and the time elapsed since the issuing date of the declaration does not exceed one year.

[14] The obligation to provide the supporting evidence will be waived in the following situations:

- if the same documents have already been provided in a previous award procedure of the European Commission, have been issued no more than one year before the date of their request by the contracting authority and are still valid at that date;
- if such evidence can be accessed by the contracting authority on a national database free of charge, in which case the economic operator shall provide the contracting authority with the internet address of the database and, if needed, the necessary identification data to retrieve the document;
- if there is a material impossibility to provide such evidence.

assessment and the evidence required, are specified in the following subsections.

Tenders submitted by tenderers not meeting the minimum levels of capacity will be rejected.

When submitting its tender each tenderer shall declare on honour that it fulfils the selection criteria for this call for tenders. The model Declaration on Honour available in ***Annex 2*** shall be used.

The initial assessment of whether a tenderer fulfils the selection criteria will be done on the basis of the submitted declaration(s).

The subsections below specify which selection criteria evidence must be provided with the tender or may be requested later, at any time during the procurement procedure, within a deadline given by the contracting authority[15].

The evidence must be provided in accordance with the applicable basis for assessment of each criterion: in case of a consolidated assessment – only by the involved entities who contribute to the fulfilment of the criterion, and in case of individual assessment – by each entity to whom the criterion applies individually.

In case not all selection criteria evidence is requested with the tender, all tenderers are **invited to prepare in advance the documentary evidence**, since they may be requested to provide such evidence within a short deadline. In any event, the tenderer proposed by the evaluation committee for the award of the contract will be requested to provide such evidence.

☝ If the tenderer does not provide valid documentary evidence within the deadlines set by the contracting authority, the contracting authority reserves the right to reject the tender. In any event, in case a tenderer proposed for the award of the contract fails to comply with the above evidence requirement, its tender will be rejected, unless there is a ground for a waiver.

Please note that a request for evidence in no way implies that the tenderer has been successful.

3.2.1. Legal and regulatory capacity

Tenderers can be natural or legal persons. Tenderers are not obliged to take a specific legal form in order to submit their tenders.

Where tenderers submit a tender through an entity, which lacks legal personality (e.g., a branch), the compliance with the exclusion criteria, selection criteria, the rules on access to procurement as well as the absence of restrictive measures shall be assessed at the level of the tenderers.

Tenderers must prove that they have the legal capacity to perform the contract and the regulatory capacity to pursue the professional activity necessary to carry out the work subject to this call for tenders.

The legal and regulatory capacity shall be proven by the evidence listed below:

[15] The obligation to provide the supporting evidence will be waived in the following situations:
- if the same documents have already been provided in a previous award procedure of the European Commission and are still up-to-date;
- if such evidence can be accessed by the contracting authority on a national database free of charge, in which case the economic operator shall provide the contracting authority with the internet address of the database and, if needed, the necessary identification data to retrieve the document.

- Proof of enrolment in a relevant trade or professional register

- The criterion applies to each member of the group individually.
- The evidence of legal and regulatory capacity must be provided with the tender.

3.2.2. Economic and financial capacity

Tenderers must comply with the following selection criteria in order to prove that they have the necessary economic and financial capacity to perform the contract.

Criterion F1	
Minimum level of capacity	Average yearly turnover of the last two financial years above EUR 100,000.
Basis for assessment	This criterion applies to the tenderer as a whole, i.e. a consolidated assessment of the combined capacities of all involved entities will be carried out.
Evidence	Copy of the profit and loss accounts and balance sheets for the last two years for which accounts have been closed from each concerned involved entity, or, failing that, appropriate statements from banks. The most recent year must have been closed within the last 18 months.

☝ All of the above-specified evidence of economic and financial capacity must be provided with the tender.

3.2.3. Technical and professional capacity

☝ With regard to technical and professional selection criteria, a tenderer may only rely on the capacities of other entities where the latter will perform the works or services for which these capacities are required. The entity on whose capacity the tenderer relies will either assume the role of a subcontractor or fall within the exceptions listed in Section 2.4.2.

Tenderers must comply with the following selection criteria in order to prove that they have the necessary technical and professional capacity to perform the contract:

Criterion T1	
The tenderer must prove experience in the design and development of interactive chatbot systems, including both frontend and backend components, and integration with web platforms.	
Minimum level of capacity	At least 2 similar projects (in scope and complexity) completed in the last three years, each with a minimum value of EUR 50,000.
Basis for assessment	This criterion applies to the tenderer as a whole, i.e. the

Criterion T1	
	consolidated assessment of combined capacities of all involved entities will be carried out.
Evidence	A list of projects meeting the minimum level of capacity. The list shall include details of their start and end date, total project amount and scope, role and amount invoiced. In case of projects still ongoing, only the portion completed during the reference period will be taken into consideration. As supporting documents for each project reference, the contracting authority may request statements issued by the clients.

Criterion T2	
The tenderer must prove experience in delivering web-based analytics dashboards, including user interaction tracking, segmentation, and reporting functionality.	
Minimum level of capacity	At least 1 similar project completed in the last three years, with a minimum value of EUR 35,000 per project.
Basis for assessment	This criterion applies to the tenderer as a whole, i.e. a consolidated assessment of the combined capacities of all involved entities will be carried out.
Evidence	A list of relevant projects with details on start and end dates, scope, total value, and functionalities delivered. The contracting authority may request contact details for verification or supporting statements issued by clients.

Criterion T3	
The tenderer must prove experience in the field of data protection compliance (Regulation (EU) 2016/679 and Regulation (EU) 2018/1725) and demonstrate the capacity to deploy AI-based solutions. The team delivering the project should include, as a minimum, the following profile: Data protection lawyer and AI Engineer.	
Minimum level of capacity	Data Protection Lawyer: A qualification in law and at least 5 years of experience in the implementation and compliance with European personal data protection law. AI Engineer: Proven hands-on experience in designing, integrating, and deploying AI-based solutions in operational environments.
Basis for assessment	This criterion applies to the tenderer as a whole, i.e. a consolidated assessment of the combined capacities of all involved entities will be carried out.
Evidence	Concise but informative curriculum vitae (CV) of each person involved in the execution of the tasks foreseen in the tender. The CVs shall demonstrate professional experience in the specific domain of this study. The Europass curriculum vitae template (available at

Criterion T3	
	https://europass.cedefop.europa.eu/documents/curriculum-vitae) shall be filled in by each person involved in the execution of the tasks foreseen in the tender. Please make sure the precise contractual link with the tenderer is clearly indicated.

☝ All of the above-specified evidence of technical and professional capacity must be provided with the tender.

☝ Involved entities (see Section 2.4) and all subcontractors, including those which do not need to be identified in the tender (see Section 2.4.2), must not be subject to professional conflicting interests which may negatively affect the contract performance.

In this regard, the tender must include a "Declaration on honour on non-conflict of interest and absence of professional conflicting interest" using the template in **Annex 7** to the tender specifications, signed by the legal representative(s) of the tenderer (sole tenderer or each group member in case of a joint tender) and declared subcontractors (if any), as well as the proposed team members/experts that will participate in the contract's implementation confirming the absence of professional conflicting interests. **This includes clearly identifying previous or ongoing relationships with entities designated under Regulation (EU) 2022/2065 as Very Large Online Platforms (VLOPs) or Very Large Online Search Engines (VLOSEs) or any of their affiliated undertakings.** For the purpose of this procurement, a professional conflicting interest is presumed to exist if, for a period of three years prior to the submission of the offer, any expert or employee working for the contractor and any authorised subcontractor(s) that is involved in the contract's implementation has represented, worked for, advised, been employed by, or been appointed as a member of the Board or other management bodies of VLOPs or VLOSEs or any of their affiliated undertakings. In such a case, the tenderer and/or subcontractors must submit mitigating measures that are being implemented or that the entity commits to implement.

The presence of conflicting interests and conflicting professional interests shall be examined during the evaluation phase based on the statements made through the Declarations on Honour and, where applicable, the commitment letters (***Annex 5.1 and Annex 5.2***). The presence of conflicting interests shall be examined also on the basis of the information about relationships with VLOPs and/or VLOSEs and any relevant mitigating measures submitted.

Where the contracting authority has established a conflict of interest or conflicting professional interests that are not sufficiently mitigated, it may conclude that the tenderer or an involved entity does not possess the required professional capacity to perform the contract to an appropriate quality standard.

In this respect, involved entities – as well as each proposed team member – and subcontractor(s) will have to disclose any professional conflicting interests that may affect the integrity of the procurement.

Further details and obligations concerning professional conflicting interests are set out in the draft contract.

3.3. Evaluation of the tenders

3.3.1. Compliance with the requirements specified in the procurement documents

By submitting a tender a tenderer commits to perform the contract in full compliance with the terms and conditions of the procurement documents for this call for tenders. Particular attention is drawn to the minimum requirements specified in Section 1.4 of these specification and to the fact that tenders must comply with applicable data protection, environmental, social and labour law obligations established by Union law, national legislation, collective agreements or the international environmental, social and labour conventions listed in Annex X to Directive 2014/24/EU.

The minimum requirements shall be observed throughout the entire duration of the contract. Compliance with these requirements is mandatory and cannot be subject to any assumptions, limitations, conditions, or reservations on the part of a tenderer.

Tenderers must declare when submitting their tenders in eSubmission whether their tenders comply with the minimum requirements specified in the procurement documents.

☝ **Tenders that are not compliant with the applicable minimum requirements shall be rejected.**

3.3.2. Award criteria

The objective of the award criteria is to evaluate the tenders with a view to choosing the most economically advantageous tender.

Tenders will be evaluated on the basis of the following award criteria and their weighting:

1. Price - 40 %

The price considered for evaluation will be the total price of the tender, covering all the requirements set out in the tender specifications.

2. Quality - 60 %

The quality of the tender will be evaluated based on the following criteria:

Technical award criterion	**Maximum score**	**Threshold**
1. **Quality and relevance of the proposed technical approach** Sub-criterion 1.1: Soundness of the proposed chatbots architecture and integration with EC infrastructure and alignment with digital sovereignty objectives (e.g. use of European-based LLMs, etc.) Sub-criterion 1.2: Proposed approach to accuracy, performance targets, validation methodology, and precision tracking across languages Sub-criterion 1.3: Proposed multilingual strategy and handling of user input categories Sub-criterion 1.4: Usability and accessibility of the chatbots interfaces	50	25

Technical award criterion	Maximum score	Threshold
Sub-criterion 1.5: Proposed measures to ensure data protection, system security, and AI guardrails *All the sub-criteria above are of equal relative importance.*		
2. **Project management, team composition and implementation plan** Sub-criterion 2.1: Clarity and feasibility of the implementation timeline and milestone planning Sub-criterion 2.2: Qualifications and relevant experience of the team proposed for this assignment Sub-criterion 2.3: Quality and robustness of the proposed risk management approach, including identification, assessment, and mitigation of technical, operational, legal, and reputational risks throughout the project lifecycle. *All the sub-criteria above are of equal relative importance.*	30	15
3. **Long-term sustainability and scalability** Sub-criterion 3.1: Strategy for future maintenance, scalability, and integration with Commission systems Sub-criterion 3.2: Potential for adaptation to other legal or policy frameworks *All the sub-criteria above are of equal relative importance.*	20	10
Total	**100**	**50**

Tenders that do not reach the respective thresholds for each individual criteria or do not reach 50% of the possible overall score for the technical evaluation (50 points minimum out of the overall total of 100 points) will be rejected.

3.3.3. Award (ranking of tenders)

Tenders shall be ranked according to the best price-quality ratio in accordance with the formula below:

score for tender X	=	cheapest price/ price of tender X	*	100	*	40 %	+	total quality score (out of 100) for all award criteria of tender X	*	60%	

Should the outcome of the formula lead to two or more tenders with the same result, the tenders with lower price will be ranked higher than the tenders with higher price.

☝ The contract shall be awarded to the tender ranked first, which complies with the minimum requirements specified in the procurement documents and is submitted by a tenderer not subject to restrictive measures, having access to procurement, not in an exclusion situation and fulfilling the selection criteria.

☝ **Detection of abnormally low tenders**

Tenderers must be aware of Point 23 of Annex I to the Financial Regulation on abnormally low tenders and of the possibility for rejection of the tender based on it.

4. FORM AND CONTENT OF THE TENDER

4.1. Form of the tender: how to submit the tender?

Tenders are to be submitted via the eSubmission application according to the instructions laid down in the Invitation letter and the eSubmission Quick Guide available at the link below:

https://wikis.ec.europa.eu/display/FTPortal/Open+procedures_EN

☝ Make sure you prepare and submit your tender in eSubmission early enough to ensure it is received within the deadline for receipt indicated under Section 5.1.12 of the contract notice and/or on Funding & Tenders Portal (F&T Portal)[16].

4.2. Content of the tender: what documents to submit with the tender?

The documents to be submitted with the tender in eSubmission are listed in ***Annex 1***.

The following requirements apply to the technical and financial tender to be uploaded in eSubmission:

- *Technical tender*

The technical tender must provide all the information needed to assess the compliance with Section 1.4 of these specifications and the award criteria. Tenders deviating from the minimum requirements or not covering all the requirements may be rejected on the basis of non-compliance and not evaluated further.

- *Financial tender.*

A complete financial tender, including the breakdown of the price, needs to be submitted. For this purpose, the Financial Model in **Annex 6** shall be used.

The financial tender shall be:

- expressed in euros. Tenderers from countries outside the euro zone have to quote their prices in euro. The price quoted may not be revised in line with exchange rate movements. It is for the tenderer to bear the risks or the benefits deriving from any variation.
- quoted free of all duties, taxes and other charges, i.e. also free of VAT.

☝ The European Union Institutions are exempt from such charges in the EU under Articles 3 and 4 of the Protocol on the Privileges and Immunities of the European Union of 8 April 1965 annexed to the Treaty on the Functioning of the European Union. Exemption is granted to the Commission by the governments of the Member States, either through refunds upon presentation of documentary evidence or by direct exemption.

In case of doubt about the applicable VAT system, it is the tenderer's responsibility to contact its national authorities to clarify the way in which the European Union is exempt from VAT.

[16] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/home

4.3. Signature policy: how can documents be signed?

Where a document needs to be signed, the signature must be either hand-written or, preferably, a qualified electronic signature (QES) as defined in Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (the *eIDAS Regulation*).

Tenderers are strongly encouraged to sign with a QES[18] all documents requiring a signature and only exceptionally to sign such documents by hand as hand-written signatures lead to an additional administrative burden for both the tenderer and the contracting authority. The originals of any hand-signed documents (other than the contract) do not need to be submitted to the contracting authority but the tenderer must keep them for a period of five years starting from the notification of the outcome of the procedure or, where the tenderer has been awarded a contract resulting from this call for tenders and the contract has been signed, the payment of the balance.

All documents must be signed by the signatories (when they are individuals) or by their duly authorised representatives.

For the following documents, when signed by representatives, tenderers must provide evidence for the delegation of the authorisation to sign:

- The Declaration on Honour of the tenderer (in case of a joint tender – the Declarations on Honour of all group members);
- (in the case of a joint tender) the Agreement/Power(s) of attorney drawn up using the model attached in ***Annex 3***).

The delegation of the authorisation to sign on behalf of the signatories (including, in the case of proxy(-ies), the chain of authorisations) must be evidenced by appropriate written evidence (copy of the notice of appointment of the persons authorised to represent the legal entity in signing contracts (together or alone), or a copy of the publication of such appointment if the legislation which applies to signatory requires such publication or a power of attorney). A document that the contracting authority can access on a national database free of charge does not need to be submitted if the contracting authority is provided with the exact internet link and, if applicable, the necessary identification data to retrieve the document.

4.4. Confidentiality of tenders: what information and under what conditions can be disclosed?

Once the contracting authority has opened a tender, it becomes its property and shall be treated confidentially, subject to the following:

- For the purposes of evaluating the tender and, if applicable, implementing the contract, performing audits, benchmarking, etc., the contracting authority is entitled to make available (any part of) the tender to its staff and the staff of other Union institutions, bodies and agencies, as well to other persons and entities working for the contracting authority or cooperating with it, including contractors or subcontractors and their staff, provided that they are bound by an obligation of confidentiality.
- After the signature of the award decision the contracting authority shall inform each tenderer

[18] See here how to apply a QES on a document exchanged with a European institution, body or agency.

who is not rejected and who make a request in writing of the name of the successful tenderer to whom the contract is awarded, the characteristics and relative advantages of the successful tender and its total financial offer amount. The contracting authority may decide to withhold certain information that it assesses as being confidential, in particular where[916].

- The contracting authority may disclose the submitted tender in the context of a request for public access to documents, or in other cases where the applicable law requires its disclosure. Unless there is an overriding public interest in disclosure[20], the contracting authority may refuse to provide full access to the submitted tender, redacting the parts (if any) that contain confidential information, the disclosure of which would undermine the protection of commercial interests of the tenderer, including intellectual property.

☝ The contracting authority will disregard general statements that the whole tender or substantial parts of it contain confidential information. Tenderers need to mark clearly the information they consider confidential and explain why it may not be disclosed. The contracting authority reserves the right to make its own assessment of the confidential nature of any information contained in the tender.

[19] For the definition of trade secrets please see Article 2 (1) of Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

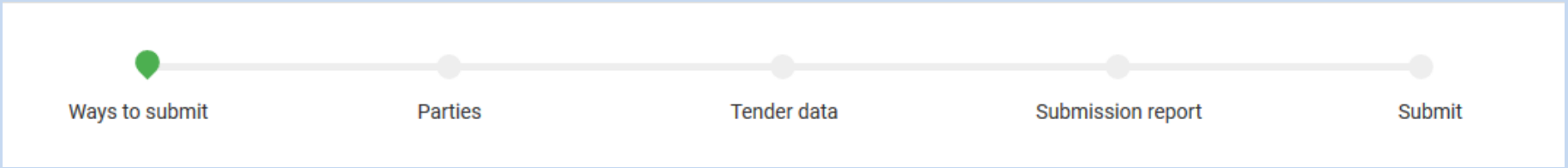
[20] See Article 4 (2) of the Regulation (EC) No 1049/2001 regarding public access to European Parliament, Council and Commission documents.

APPENDIX: LIST OF REFERENCES

Award criteria	See Section 3.4
Contracting authority	See Section 1.1
Entities on whose capacities the tenderer relies to fulfil the selection criteria	See Section 2.4.3
EU Validation services	See Section 2.3 EU Grants and Tenders Rules on Legal Entity Validation, LEAR appointment and Financial Capacity assessment
Exclusion criteria	See Section 3.1
Financial Regulation	Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council of 23 September 2024 on the financial rules applicable to the general budget of the Union (recast) (OJ L, 2024/2509, 26.9.2024, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).
Group leader	See Section 2.4.1
Group member	See Section 2.4.1
Identified subcontractors	See Section 2.4.2
Involved entities	See Section 2.4
Joint tender	See Section 2.4.1
Participant Register	See Section 2.3 https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/how-to-participate/participant-register
Selection criteria	See Section 3.2
Sole tenderer	See Section 2.4
Subcontracting/subcontractor	See Section 2.4.2
Treaties	The EU Treaties: https://europa.eu/european-union/law/treaties_en

ANNEXES

Annex 1. List of documents to be submitted with the tender or during the procedure

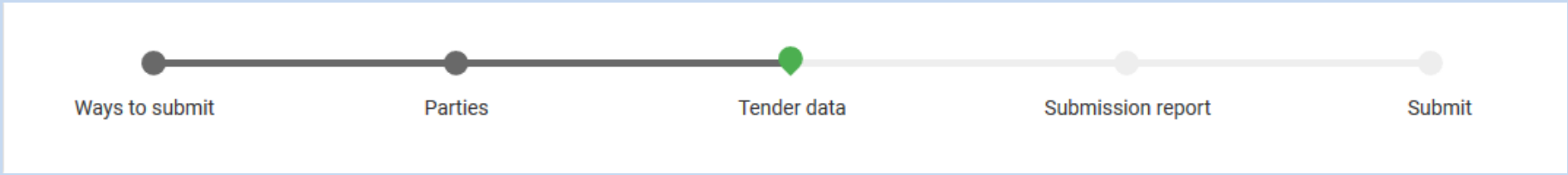
Description	Sole tenderer	Joint tender		Identified Subcontractor	Entity on whose capacity is being relied (that is not subcontractor)	When and where to submit the document?	Instructions for uploading in eSubmission (if applicable)	
		Group leader	Group member				How to name the file?	Where to upload?
1. Identification and information about the tenderer. *eSubmission view* 								
Declaration on Honour on Exclusion and Selection Criteria (see Section 3.1) *model in Annex 2*	☒	☒	☒	☒	☒	With the tender in eSubmission	'Declaration on Honour'	With the concerned entity under 'Parties' →'Identification of the participant' →'Attachments'→'Declaration on Honour'. For entities that are not subcontractors and on whose capacity the tenderer relies to fulfil the selection criteria, the document must be uploaded in the section of the sole tenderer or group leader: →'Identification of the participant' →'Attachments'→'Other documents'.
Evidence that the person	☒	☒	☒			With the tender	'Authorisation to	With the concerned entity

Description	Sole tenderer	Joint tender		Identified Subcontractor	Entity on whose capacity is being relied (that is not subcontractor)	When and where to submit the document?	Instructions for uploading in eSubmission (if applicable)	
		Group leader	Group member				How to name the file?	Where to upload?
signing the documents is **an authorised**[0] of the entity[27] (see Section 4.3)						in eSubmission	sign documents'	under 'Parties' →'Identification of the participant' →'Attachments'→'Other documents'.
Agreement/Power of attorney (see Section 2.4.1) *model in Annex 3*		☒	☒			With the tender in eSubmission	'Agreement Power of attorney'	In the group leader's section under 'Parties' →'Identification of the participant' →'Attachments'→'Other documents'.
List of identified subcontractors (see Section 2.4.2) *model in Annex 4*	☒	☒				With the tender in eSubmission	'List of identified subcontractors'	In the sole tenderer's or the group leader's section under 'Parties' →'Identification of the participant' →'Attachments'→'Other documents'.
Commitment letter (see Section 2.4.2 and 2.4.3)				☒ *(model in Annex 5.1)*	☒ *(model in Annex 5.2)*	With the tender in eSubmission	'Commitment letter'	With the concerned entity under 'Parties' →'Identification of the

[20] A document that the contracting authority can access on a national database free of charge does not need to be submitted if the contracting authority is provided with the exact internet link and, if applicable, the necessary identification data to retrieve the document.

Description	Sole tenderer	Joint tender		Identified Subcontractor	Entity on whose capacity is being relied (that is not subcontractor)	When and where to submit the document?	Instructions for uploading in eSubmission (if applicable)	
		Group leader	Group member				How to name the file?	Where to upload?
								participant' →'Attachments'→'Other documents'.
Evidence of non-exclusion (see Section 3.1)	☒	☒	☒	☒	☒	Tenderers (sole tenderers/all group members in case of a joint tender) must provide the evidence when requested by the contracting authority and, in any event, if a tenderer is successful, before the award of the contract. Subcontractors and entities on whose capacity a tenderer relies to fulfil the selection criteria must provide the evidence only upon request by the contracting authority.	n.a.	n.a.
Evidence of legal existence and status (see Section 2.3)	☒	☒	☒			Only upon request by *the EU Validation services* At any time during the procedure In the Participant Register	n.a.	n.a.
Evidence of legal capacity (see Section 3.2.1)	☒	☒	☒			With the tender in eSubmission	No specific requirements how to name the file(s).	With the concerned entity under 'Parties' →'Identification of the participant' →'Attachments'→'Legal and regulatory capacity'.

Description	Sole tenderer	Joint tender		Identified Subcontractor	Entity on whose capacity is being relied (that is not subcontractor)	When and where to submit the document?	Instructions for uploading in eSubmission (if applicable)	
		Group leader	Group member				How to name the file?	Where to upload?
Evidence of economic and financial capacity F1 (see Section 3.2.2)	**The documents must be provided only by the involved entities which contribute to reaching the minimum capacity level for criterion F1**					With the tender in eSubmission	'Balance sheet entity year' 'Profit Loss Account entity year'	With the group leader or the sole tenderer under 'Parties' →'Identification of the participant' →'Attachments'→'Economic and financial capacity'.
Evidence of technical and professional capacity T1 (see Section 3.2.3)	**The documents must be provided only by the involved entities which contribute to reaching the minimum capacity level for criterion T1**					With the tender in eSubmission	'Project reference No.1' 'Project reference No.2' ….	With the group leader or the sole tenderer under 'Parties' →'Identification of the participant' →'Attachments'→'Technical and professional capacity'.
Evidence of technical and professional capacity T2 (see Section 3.2.3)	**The documents must be provided only by the involved entities which contribute to reaching the minimum capacity level for criterion T1**					With the tender in eSubmission	'Project reference No.1' 'Project reference No.2' ….	With the group leader or the sole tenderer under 'Parties' →'Identification of the participant' →'Attachments'→'Technical and professional capacity'.
Evidence of technical and professional capacity T3 (see Section 3.2.3)	**The documents must be provided only by the involved entities which contribute to reaching the minimum capacity level for criterion T1**					With the tender in eSubmission	'CV No.1' 'CV No.2' ….	With the group leader or the sole tenderer under 'Parties' →'Identification of the participant' →'Attachments'→'Technical and professional capacity'.

Description	Sole tenderer	Joint tender		Identified Subcontractor	Entity on whose capacity is being relied (that is not subcontractor)	When and where to submit the document?	Instructions for uploading in eSubmission (if applicable)	
		Group leader	Group member				How to name the file?	Where to upload?
Declaration on non-conflict of interest and absence of professional conflicting interests – <u>to be supplied also for each proposed expert/ proposed team member</u> *Model in Annex 7*	☒	☒	☒	☒	☒	With the tender in eSubmission	'Declaration on non-COI'	In the sole tenderer's or the group leader's section under 'Parties' →'Identification of the participant'
2. Tender data. *eSubmission view*  ***Failure to upload the following documents in eSubmission will lead to rejection of the tender.***								
Technical tender (see Section 4.2)	☒	☒				With the tender in eSubmission	'Technical tender'	Under section 'Tender Data' →'Technical tender'
Financial tender (see Section 4.2) *model in Annex 6*	☒	☒				With the tender in eSubmission	'Financial tender'	Under 'Tender Data' →'Financial tender'

Annex 2. Declaration on Honour on exclusion and selection criteria

Annex 2 is published as a separate document

Annex 3. Agreement/Power of attorney

Annex 3 is published as a separate document

Annex 4. List of identified subcontractors and proportion of subcontracting

Annex 4 is published as a separate document

Annex 5.1. Commitment letter by an identified subcontractor

Annex 5.1 is published as a separate document

Annex 5.2. Commitment letter by an entity on whose capacities is being relied

Annex 5.2 is published as a separate document

Annex 6. Financial tender form

Annex 6 is published as a separate document

Annex 7. Declaration on non-conflict of interest and absence of professional conflicting interest

Annex 7 is published as a separate document