

Terms of Reference (ToR) for the procurement of IT services

CONFIDENTIAL

Project title:	Processing
Regional Cooperation for EU Integrations (RCEI) - EU4Digital	number/cost centre:
Country:	G-012362-003
West Balkans	Transaction number:
Works/services to be put out to tender:	81322924
Technical and Advisory Services for Developing and Piloting an Interoperable Digital Wallet based Cross-Border e-Service	

0. Abbreviations	3
1. Context.....	4
1.1 The Company	4
1.2 Project Background	4
1.3 Objective of the commission/subject of the procurement.....	5
2. Tasks to be performed by the contractor	6
2.1 Term	6
2.2 Objectives, indicators, work packages, milestones	6
2.2.1 Monitoring, Reporting, and Communication.....	9
2.2.2 Knowledge and Learning.....	10
2.2.3 Backstopping	10
2.3 Further specifications/general conditions.....	10
3. Responsibilities of the contractor.....	11
3.1 Work package 1: Phase 1 - Kick-off & Inception Phase.....	11
3.2 Work package 2: Phase 2 - Technical Design, Co-Development, and Regional Deployment.....	12
3.3 Work package 3: Phase 3 - Evaluation, Reporting, and Capacity Building	12
4. Term, schedule and milestones	13
5. Data Protection & Information Security	14
6. Technical and methodological concept.....	16
6.1 Assessment of Requirements (section 1.1 of the assessment grid).....	16
6.2 Project Management and Development Methodology (section 1.2 of the assessment grid).....	16
6.3 Operational Plan/Personnel Assignment Plan (section 1.3 of the assessment grid).....	16
6.4 Test and Documentation Concept (section 1.4 of the assessment grid)	17
6.5 Additional Requirements (section 2 of the assessment grid)	17
7. Human Resource.....	17
7.1 Expert 1: Team Leader/Project Manager (Section 3.1 of the assessment grid) ..	18
7.2 Expert 2: Solution Architect (Section 3.2 of the assessment grid).....	19
7.3 Expert 3: ICT Business Analyst (Section 3.3 of the assessment grid).....	20

7.4	Expert 4: Technical Lead / Integration Engineer (Section 3.4 of the assessment grid).....	21
7.5	Expert 5: Data Protection & Compliance Expert (Section 3.5 of the assessment grid).....	22
7.6	Expert 6: Legal / Trust Services Advisor (Section 3.6 of the assessment grid) ...	23
7.7	Expert 7: UI/UX & Accessibility Specialist (Section 3.7 of the assessment grid) .	24
7.8	Expert 8: Training & Capacity Building Expert (Section 3.8 of the assessment grid).....	25
7.9	Expert 9: DevOps / Cybersecurity Specialist (Section 3.9 of the assessment grid)	26
8.	Costing requirements	27
8.1	Assignment of experts	27
8.2	Travel expenses.....	28
8.2.1	Travel – sustainability considerations	28
8.2.2	Travel expense requirements	28
8.3	Workshops, training	29
8.4	Flexible remuneration.....	29
9.	Requirements on the format of the tender	29

0. Abbreviations

API	Application programming interface
BMF	Federal Ministry of Finance
BMZ	Federal Ministry of Economic Cooperation and Development
CV	Curriculum vitae
eDIHs	EU-integrated network of European Digital Innovation Hub
eFTI	Electronic freight transport information architecture
ERD	Entity relationship diagram
EVB-IT	Supplementary Terms and Conditions for the Procurement of IT Services
GIZ	Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH
GTC	General Terms and Conditions
GWB	German Competition Act
KOMP	Cost per output monitoring and forecast
LoI	Letter of intent
MoU	Memorandum of Understanding
MSMEs	Medium-sized enterprises
OSS	Open-source software
RCEI	Regional Cooperation for EU Integration
RMO	Risk Management Office
SaaS	Software-as-a-service
ToR	Terms of Reference
ToRs	Terms of reference
VgV	German Ordinance on the Award of Public Contracts
WB6	Six West Balkan (6) Countries

1. Context

1.1 The Company

The Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH supports the German Federal Government in achieving its objectives in the field of international cooperation for sustainable development and international education. The company is active in several fields: economic development and employment; governance and democracy; peacebuilding, security, reconstruction and civil conflict transformation; food and nutrition security, health, basic education, environmental protection, resource conservation and climate change mitigation.

GIZ operates in some 120 countries worldwide and sends experts and managers to projects and programmes. A high percentage of these partner countries are marked by fragile statehood, violence and risks for individual safety and security. GIZ is responsible not only for its own staff members but also for the safety and security of partners, consultants and other involved parties.

1.2 Project Background

The project Regional Cooperation for EU Integration (RCEI) aims at strengthening regional cooperation among Western Balkan authorities in the EU accession process and thus promoting joint action by state actors. It initiates and promotes sustainable regional cooperation among the six Western Balkan countries (WB6) through relevant measures and instruments which aim to consolidate the EU accession process in selected domains of action. This approach derived from the facts that, on one hand Albania, Bosnia and Herzegovina, Kosovo, North Macedonia, Montenegro, and Serbia, have made EU membership one of their highest national priorities and on the other hand, the European Commission has declared regional cooperation to be a key condition for joining the EU. The countries of the WB6 have made different progress in the accession process; however, they face numerous common challenges, particularly in the areas of economic and political reform, and reforming public administration.

In addition to the existing implementation structure - networks, the RCEI established structures that will support implementation of measures within the project EU4Digital - An accelerated digital transition for the Western Balkans – Phase I. The EU4Digital project became integral part of existing RCEI project, and it is jointly financed by the European Union and the Federal Ministry of Economic Cooperation and Development (BMZ). The implementation has started as of 1st September 2024 and will last for three years. Phase II is envisioned to be developed as a follow-on project in the course of year 2026.

The overall objective of the EU4Digital initiative is to enhance digital connectivity and digital transition of the Western Balkan region, and an accelerated integration of the Western Balkans into the EU Digital Single Market.

The Project consists of three main components, and it aims to achieve the following specific objectives:

1. Development of secure and sustainable digital and telecom infrastructure across the region rolled out.

2. Interoperability and e-Governance of public services on the central and/or regional levels, and between the Western Balkans and the EU enhanced.
3. Digitalization of businesses in the Western Balkans supported.

Establishment of a regional initiative on providing free public Wi-Fi networks in WB municipalities as well as better preparedness of WB governments to establish digital infrastructure project pipelines will be in the focus within the component/specific objective 1. For the component/specific objective 2, the project will work on developing regional framework for cross-border mutual recognition of trust services as well as it will seek to pilot a regional interoperable e-services. In addition, the Project will provide support to WB institutions for fulfilling prerequisites for single digital gateway. Within the specific objective 3., the project will support the digitalization of the transport and logistics sector by preparing selected elements of the electronic freight transport information architecture for testing – eFTI. Also, the project will establish a strong foundation for broader digitalization of micro, small and medium-sized enterprises (MSMEs) by building a strong WB6 wide and EU-integrated network of European Digital Innovation Hub (eDIHs).

Main partners are governments across the Western Balkans along with the ministries responsible for overseeing the digital transformation of their economies or in the case of component three it is the ministries responsible for transport sector. These ministries often have subordinate organizations, such as national IT agencies and SME promotion agencies, that will also be instrumental as partners.

By bringing together this network of partners, the RCEI will aim to create a comprehensive and inclusive digital transformation initiative across the Western Balkans.

1.3 Objective of the commission/subject of the procurement

The Western Balkan Six (WB6) economies, Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia, and Serbia, during the past years have made substantial progress in building national digital public infrastructures. All six countries have established national interoperability platforms that enable secure data exchange between public sector institutions (Note: While Bosnia and Herzegovina have established an interoperability framework, its full operationalization remains limited or under development in some areas). These platforms are typically managed by central government bodies or national IT agencies and serve as the backbone for the digitalization of administrative processes and the delivery of user-oriented e-services.

Across the region, interoperability frameworks are already being used to connect population registries, civil status records, tax systems, health institutions, business registers, and social welfare databases. These national frameworks help automate and simplify citizen and business interactions with government, ranging from online registration of businesses and access to social benefits, to secure electronic payments and using digital certificates.

Furthermore, WB6 countries have developed and launched various eGovernment services for both individuals and businesses, with growing levels of service maturity. Many of these services have moved beyond basic information provision to include transactional features and personalized user experiences. National service portals, electronic registers, and backend digital registries now allow for significant reductions in paperwork, waiting times, and administrative costs. The continued development of these services has also led to growing demands for cross-border functionality and mutual recognition of digital credentials.

Building on this foundation, all WB6 economies have also initiated national digital wallet projects. These efforts aim to support secure, user-controlled access to personal data, credentials, and trust services, in line with the EU Digital Identity Framework and the revised eIDAS 2.0 Regulation. However, the maturity of these wallet initiatives varies significantly across the region, both in terms of technical readiness and legal frameworks.

As part of the implementation of the second specific objective of EU4Digital initiative – Interoperability and e-Governance of public services on the central and/or regional levels, and between the Western Balkans and the EU enhanced, **this assignment aims to support the development and regional pilot deployment of an interoperable digital service prototype, leveraging either:**

- **A wallet-based model, or**
- **A mutual recognition-based model, depending on the maturity and readiness of national ecosystems.**

The main objective of this assignment is to engage a qualified IT Solution Provider or Technology Service Provider to deliver expert technical conceptualization, support and implementation, project coordination, and stakeholder facilitation across the WB6 economies. The contractor will lead the co-development, testing, and deployment of an interoperable digital service prototype, while ensuring alignment with national priorities and EU digital policy frameworks. In parallel, the contractor will support institutional capacity building and knowledge transfer to enable long-term sustainability and regional scalability of the solution.

2. Tasks to be performed by the contractor

2.1 Term

The expected term of the contract for services must be specified in the 'Special terms and conditions of contract'. The definitive term and service delivery period are set out in the contract award notification.

2.2 Objectives, indicators, work packages, milestones

Scope of Work and Phased Implementation

The assignment is structured into three interconnected phases, each serving a distinct purpose in the development of the lifecycle of the regional prototype. The contractor shall deliver its services through the following integrated phases:

- **Phase 1: Inception and Review**
- **Phase 2: Technical Design, Co-Development, Testing and Regional Deployment**
- **Phase 3: Evaluation, Reporting, and Capacity Building**

Phase 1: Inception and Review

This phase establishes a common understanding of the assignment, validates the findings of prior assessments, and refines the technical and operational roadmap for implementation. The contractor reviews the assessment reports prepared under a previous phase, identifies residual gaps, and ensures all technical, legal, and institutional preconditions are met before proceeding to co-development.

Under this phase, the contractor shall:

- Review and validate the outcomes of the regional assessment and readiness studies for WB6 digital ecosystems and digital wallet maturity.
- Identify gaps, inconsistencies, or dependencies that may affect technical design or deployment.
- Conduct targeted consultations with national focal points and relevant institutions to confirm priorities and validate the selected cross-border use cases.
- Develop a consolidated implementation roadmap detailing architecture assumptions, development milestones, and stakeholder coordination mechanisms.
- Prepare inception deliverables, including a refined work plan, updated stakeholder map, and governance structure.

Phase 2: Technical Design, Co-Development, and Regional Deployment

This phase focuses on the co-creation, design, and development of the regional prototype for selected cross-border e-services, ensuring interoperability and alignment with EU frameworks such as eIDAS 2.0 and the European Digital Identity Wallet initiative. The contractor will facilitate technical collaboration in developing the prototype and test it under controlled and live conditions.

Under this phase, the contractor shall:

1. Facilitate joint co-creation sessions with WB6 stakeholders (i.e. ministries, departments and IT service providers) to confirm technical and functional specifications based on validated use cases.
2. Design and detail the technical target architecture and interoperability model, ensuring compatibility with both wallet-based and mutual recognition approaches (federation/interoperability-based models), as well as the prototype and a roadmap leading from there to the target architecture.
3. Coordinate and co-develop the prototype in close collaboration with national IT service providers and platform owners, ensuring alignment with agreed design principles, integration protocols (e.g. REST APIs, OAuth2, OpenID Connect), and cybersecurity requirements (e.g. NIS2, ISO/IEC 27001).
4. Support the co-development and implementation of the core functionalities of the cross-border service in close collaboration with national IT providers and WB6 stakeholders. These functionalities, to be defined through a joint specification process, may include (but are not limited to):
 - a. Secure user authentication
 - b. Data exchange and validation
 - c. Consent management
 - d. Logging and auditing transactions
 - e. Credential issuance and verification
 - f. Transaction processing is supported by qualified trust services, in compliance with eIDAS 2.0 and other relevant EU frameworks.
5. Support the integration of the prototype with at least one national digital wallet per WB6 economy (where technically and institutionally feasible), in collaboration with national wallet and interoperability platform providers. This integration should align with core interoperability principles as defined by the European Interoperability Framework (EIF), eIDAS 2.0, and the European Digital Identity Wallet Architecture

Reference Framework (ARF), while adapting to the differing levels of ecosystem maturity across the region.

6. Conduct pilot testing in both sandbox and existing live environments, in coordination with national IT providers and authorities. Testing shall simulate real-world conditions to validate system behavior, performance, user experience, and compliance, while structured feedback is collected for iterative refinement of the solution.
7. Upon successful completion of technical pilot testing, carry out structured user testing with selected institutions and user groups in participating in WB6 economies. Execute previously defined test cases to assess functionality, usability, accessibility, and cross-border operability from an end-user perspective. Proceed with regional deployment only after receiving validation and confirmation of readiness from national technical providers.
8. Coordinate with national IT partners to refine and stabilize the solution based on feedback from testing and validation stages, resolving technical and functional issues, and supporting stakeholder approval of the final version.
9. Support the regional deployment of the prototype for live testing in collaboration with national IT providers and participating institutions, using existing operational environments; monitor system performance, collect usage data, and gather structured feedback under real service conditions.
10. Finalize and deliver, in collaboration with national IT partners, a stable and production-ready version of the prototype suitable for broader institutional adoption
11. Deliver a stable, fully functional prototype ready for broader institutional adoption.

Note (on bullet point 3): As national interoperability platforms and digital wallets are operated by designated vendors in each WB6 economy, the contractor will act as a co-developer and technical integrator in collaboration with these actors. The full development of the prototype depends on coordination with national-level providers and may require adapting to differing technical environments and governance models.

Note (on bullet point 4): Implementation will take place through a co-development approach, where the contractor works alongside national IT service providers responsible for each WB6 interoperability platform. The contractor's role includes coordination, technical design support, joint testing, and quality assurance, but not exclusive end-to-end development.

Note (on bullet point 5): The contractor will not perform direct integration activities independently but will support and coordinate integration efforts with national IT teams and wallet providers through technical guidance, interface specification, and validation.

Note (on bullet point 6): Live environments refer to operational national interoperability and service platforms managed by WB6 authorities; no new infrastructure is expected to be developed or provided by the contractor.

Phase 3: Evaluation, Reporting, and Capacity Building

This phase ensures that lessons learned, and knowledge gained are captured, shared, and institutionalized. It strengthens the capacity of WB6 stakeholders to maintain, extend, and replicate the solution independently, supporting alignment with national digital strategies and EU integration frameworks.

Under this phase, the contractor shall:

1. Conduct a comprehensive evaluation of the prototype lifecycle, including performance, usability, interoperability, and regulatory compliance.
2. Prepare technical and functional documentation for maintenance, scalability, and replication in additional sectors or use cases.
 - a. Detailed technical documentation of the developed prototype and its architecture
 - b. Summary of lessons learned, including challenges encountered and how they were resolved
 - c. A scalability roadmap outlining how the solution could be extended to additional use cases, sectors, or services
3. Support the structured transfer of knowledge (i.e. repositories, training programs and mentoring), tools, and documentation to ensure that participating WB6 economies are fully capable of maintaining, expanding, and adapting the prototype independently after project completion.
4. Deliver targeted capacity-building workshops for public institutions and technical teams in each WB6 economy, aimed at strengthening knowledge and skills related to interoperable digital services, digital identity, and trust frameworks.
5. Facilitate strategic planning sessions with key stakeholders to explore integration of the prototype into national digital transformation agendas and its alignment with broader EU frameworks such as eIDAS 2.0 and Single Digital Gateway Regulation (EU) 2018/1724.
6. Produce a final evaluation and scalability roadmap with actionable recommendations for sustainability and institutionalization.

2.2.1 Monitoring, Reporting, and Communication

The contractor plays an active role in **results-based monitoring**, in line with the objectives, indicators, and milestones defined in **Section 2.2**. Monitoring shall track:

- Progress against work plan and deliverables.
- Achievement of defined indicators and milestones.
- Emerging results within and beyond the contractor's sphere of responsibility.
- Identified risks and mitigation actions.

Reporting Requirements

All reports shall be submitted electronically in **English** and must follow GIZ formatting and content guidelines.

Report	Timing / Length	Main Content
Inception Report	Within 4 weeks of contract signature (max. 10 pages)	Understanding of assignment, refined methodology, stakeholder coordination, timeline confirmation
Interim Reports	Month 4 and Month 8 (max. 8–10 pages each)	Progress toward outputs and indicators, issues encountered, next steps
Final Report	Month 10 (max. 15–20 pages)	Lessons learned, recommendations, scalability options

Report	Timing / Length	Main Content
Quarterly Briefs (optional)	As agreed,	Short progress updates for coordination

The contractor will also participate in **regular virtual coordination meetings** (monthly or as agreed) with GIZ and national focal points and provide ad-hoc updates when major milestones are reached, or challenges arise. A **final virtual debriefing** will be held upon project completion.

2.2.2 Knowledge and Learning

The contractor contributes to **knowledge management and learning** across the WB6 region and within GIZ by:

- Documenting lessons learned and best practices from prototype co-development and deployment.
- Sharing technical insights and tools/templates developed under the assignment.
- Participating, when feasible, in regional or EU-level learning events (e.g., eIDAS 2.0 or EU digital identity forums).
- Supporting cross-project knowledge exchange within GIZ's digital governance and data policy portfolio.

2.2.3 Backstopping

The contractor shall ensure effective backstopping arrangements in accordance with GIZ's General Terms and Conditions.

Backstopping shall include:

- Technical and administrative oversight of project staff.
- Quality assurance of deliverables.
- Continuous coordination with GIZ and adaptation to evolving framework conditions.
- Ensuring continuity of operations and institutional memory.

Where relevant, the contractor may offer **value-added backstopping services**, such as:

- Ad-hoc expert advice or peer review of digital tools or prototypes.
- Targeted support to national stakeholders on specific implementation challenges.

2.3 Further specifications/general conditions

Safeguards and gender measures with specific reference to services:

In order to promote gender equality and avoid or mitigate possible unintended negative impacts in its area of responsibility, the contractor should implement the following measures:

- **Gender equality:** The contractor should ensure gender-sensitive planning and implementation. Teams must reflect gender balance where possible, and outputs should account for gender-specific needs and impacts.

- **Environmental protection and climate action (climate change mitigation/adaptation):** Services must be implemented in a manner that supports environmental sustainability and addresses potential climate change risks (mitigation and/or adaptation).
- **Conflict and context sensitivity:** The contractor must ensure that activities are tailored to the local context, considering potential risks related to political or social tensions.
- **Human rights:** All activities must respect human rights standards. The contractor must avoid any actions that could infringe upon the rights of affected groups or individuals.

3. Responsibilities of the contractor

The contractor will deliver the following services and work packages (along with the corresponding milestones). The work packages have no chronological order and can also be implemented on an integrated basis, depending on the development methodology:

The contractor shall be responsible for delivering the following outputs, structured according to the three phases of implementation. All deliverables must be submitted electronically in English. Translations into local languages may be requested on a case-by-case basis in coordination with national stakeholders and agreed upon with GIZ.

The contractor shall be responsible for achieving the following objectives and deliverables, structured according to the implementation phases.

Objectives

- Operationalize a regional cross-border e-service prototype aligned with eIDAS 2.0 principles.
- Strengthen interoperability and trust service capacities across the WB6 economies.
- Enable national institutions to sustain and expand the prototype beyond the project's duration.

3.1 Work package 1: Phase 1 - Kick-off & Inception Phase

At the start of the project, the contractor and GIZ clarify the expectations for the cooperation arrangement, the technical platform for cooperation, details of the relevant responsibilities and the project schedule. The first meeting also allows substantive questions to be clarified regarding the issues, defined objectives, requirements and other contextual information.

To ensure a shared understanding of project scope, methodology, and timeline, the contractor shall prepare and submit the following within the first 2–4 weeks of contract signature:

- **Kick-off Meeting**, to discuss the start of the project and the deliverable and clarification.
- **Inception report**, (methodology, implementation roadmap, validation of assessment findings, stakeholder engagement plan).
- **Detailed work plan and implementation schedule**, including timelines, resource allocation, and proposed sequencing of activities across the three phases.

Transaction number: 81322924

- **Stakeholder engagement and communication plan**, detailing how coordination with WB6 institutions, national focal points, and the GIZ team will be ensured throughout the assignment.
- **Refined compliance roadmap**, (cybersecurity, data protection, trust services).

3.2 Work package 2: Phase 2 - Technical Design, Co-Development, and Regional Deployment

Outcomes to be delivered by the contractor:

- **Technical architecture and interoperability design document** for the cross-border e-service(s) prototype, detailing system components, integration models, and alignment with wallet-based and mutual recognition approaches.
- **Validated Cross-Border Use Case Specifications**: Facilitation of validation and prioritization of four pre-identified use cases (Birth Certificate Integration, Digital Work Permits, Personal Identification Data, Vehicle Registration), with technical and functional specifications for the selected pilot including Interoperability and integration model.
- **Fully functional prototype**, integrated with at least one national digital wallet in each WB6 economy (where technically and institutionally feasible).
- **Technical documentation of implemented core functionalities**, including secure user authentication, credential issuance and exchange, and trust-enabled transaction processing.
- **Pilot testing report** covering both sandbox and live testing environments, including test cases, user feedback, performance assessments, and identified technical or usability issues.
- **Final deployment package**, including updated prototype, technical fixes, and user documentation.

3.3 Work package 3: Phase 3 - Evaluation, Reporting, and Capacity Building

Outcomes to be delivered by the contractor:

- **Final evaluation report**, covering the entire prototype lifecycle, including key achievements, challenges encountered, lessons learned, and the prototype's impact on cross-border interoperability and institutional collaboration.
- **Scalability roadmap and strategic recommendations** outlining options for extending the prototype to additional services, sectors, or WB6 institutions, and for integrating it into national and regional digital transformation agendas.
- **Technical documentation** providing implementation details, system architecture, configuration guidance, and operational instructions to enable further development and independent maintenance by national teams.
- **Training and capacity-building materials**, tailored to public institutions and technical teams, including workshop agendas, presentations, hands-on exercises, and supporting guidance documents for knowledge transfer and skills development.

Transaction number: 81322924

4. Term, schedule and milestones

The expected term of the contract is 22 months.

The following dates/deadlines apply for achieving the milestones:

Milestones	Delivery date/period	Responsible
Kick-off, Inception & Validation	(1–2 months) after contract start	• Inception report • Detailed work plan and implementation schedule • Stakeholder engagement and communication plan • validated roadmap • governance model
Functional & Technical Design	(3 months) after Inception & validation	• Functional and technical concept for the selected e-service(s) prototype • Technical architecture and interoperability design document • Governance model, risk mitigation strategy, and compliance roadmap
Technical guidance and advisory support during the deployment phase	(6 months) after Functional & Technical Design	• Provision of technical guidance and advisory support during the deployment phase with at least one national wallet per WB6 economy (where feasible) • Documentation of implemented functionalities, including authentication, credential exchange, and transaction processing
Testing & Validation Report	(3 months) after Prototype Development & Deployment	• Prototype deployed in sandbox/live • Pilot testing report • Final deployment package
Evaluation & Capacity Building	(6 month) after Testing & Validation Report	• Final evaluation report with lessons learned and strategic recommendations

		• Technical documentation and handover package • Training and capacity-building materials for workshops conducted across WB6
--	--	---

5. Data Protection & Information Security

The contractor shall comply with the provisions on data protection and information security as stipulated in the current version of GIZ's General Terms and Conditions of Contract.

The performance of the contract may be associated with the processing of personal data by the contractor, such as (but not limited to) names and contact information. In such cases, the contractor shall act as an independent DATA CONTROLLER and must alone comply with ALL applicable data protection obligations, including those stemming from regional and local laws. The contractor shall process personal data only when a given goal cannot be reasonably attained without such data. The data protection principles such as lawfulness, data minimization, accuracy, purpose limitation, storage limitation, transparency, integrity and confidentiality, and accountability, as well as the numerous rights of the data subject must be paid due attention. The GIZ is NOT in any way responsible for such processing.

Whenever the contractor executes the instructions of a partner to the GIZ regarding such processing, the partner shall be the data controller, and the data processing shall be carried out in accordance with the partner's instructions as well as laws and standards to which it is subject.

If the contractor is not subject to the GDPR and the applicable laws do not contain any explanation on the data protection principles and rights mentioned here, the definitions and meanings provided by the GDPR (Regulation (EU) 2016/679) should be considered.

Data protection by design and by default

The digital tool developed or upgraded on behalf of a local partner of GIZ must meet the highest data protection standards, especially those relating to data protection by design and by default, as stated in Annex "Data protection standards for developing digital tools meant for GIZ's partners". The contractor is therefore required to inform GIZ if any applicable national requirement is incompatible with the provisions of this annex. We equally recommend the partner to conclude data protection agreements with the hosting service provider(s) and the maintenance service provider(s), where applicable. The GIZ would be available to support the partner whenever need arises.

When the GIZ hires a contractor to develop or upgrade a data processing system (platform, website, app etc.) on behalf of a local partner, who determines the purposes and means of the data processing activity, the GIZ does not bear ANY responsibility for such processing. Although the GIZ builds such systems in conformity with the highest data protection standards, however, its responsibilities end with the handing over of the systems to the partner. As a data controller, the partner must ALONE comply with all local and regional laws applicable to such processing (including the GDPR, where applicable). Consequently, the data protection principles such as lawfulness, data minimization, accuracy, purpose limitation, storage limitation, transparency, integrity and confidentiality, and accountability, as

well as the numerous rights of the data subject should be paid due attention. We equally recommend the partner to conclude data protection agreements with the hosting service provider(s) and the maintenance service provider(s), where applicable. The GIZ would be available to support the partner whenever need arises.

Given the project's scope — including assessment, design, and co-development of cross-border digital services and wallet-integrated prototypes — the following requirements are mandatory:

- **Regulatory Compliance:** The contractor must ensure full compliance with the EU General Data Protection Regulation (GDPR), eIDAS 2.0 Regulation, and applicable national data protection laws within the Western Balkans economies.
- **Data Protection by Design and by Default:** All digital components and prototypes must be designed with privacy and security principles embedded throughout their lifecycle, from concept to deployment and maintenance.
- **Data Protection Impact Assessment (DPIA):** Prior to implementing or testing any solution that involves personal data, a DPIA shall be conducted in coordination with GIZ to identify and mitigate data protection risks.
- **Information Security Standards:** The contractor shall apply recognized information security frameworks (e.g., ISO/IEC 27001 or equivalent) and ensure secure data transmission, storage, and access management in all environments (sandbox and live).
- **Access Control and Authentication:** Appropriate role-based access control and secure authentication mechanisms must be implemented for all users, administrators, and partner systems.
- **Incident Management:** The contractor must establish and maintain procedures for detecting, reporting, and responding to any data breach or security incident in line with GDPR Article 33 obligations and GIZ's internal reporting procedures.
- **Third-Party Compliance:** All subcontractors, partners, or vendors engaged in the assignment must comply with the same data protection and information security obligations, including confidentiality and secure data handling.
- **Data Retention and Deletion:** Personal and sensitive data collected or processed during the assignment must be retained only as long as necessary for project purposes and securely deleted thereafter, in accordance with GIZ's data handling requirements.
- **Confidentiality and Secure Communication:** The contractor shall ensure encrypted communication channels, secure storage of all project data, and strict confidentiality of sensitive project-related information.

The contractor is fully responsible for ensuring that all project activities, tools, and outputs uphold these standards, safeguarding the integrity and trustworthiness of the digital solutions developed under this assignment.

6. Technical and methodological concept

In the conceptual design of the tender (technical and methodological approach, project management, if necessary other requirements), the tenderer is required to take specific objectives and requirements into consideration and describe them as explained below.

6.1 Assessment of Requirements (section 1.1 of the assessment grid)

- The tenderer must evaluate the objectives and technical requirements of the project, identifying **potential technical and non-technical challenges** that could arise during implementation.
- The evaluation should include an analysis of system complexity, integration with existing infrastructure, and the scalability of the prototype / pilot.
- The tenderer must propose solutions to overcome identified challenges, ensuring that the project stays on track and aligns with the goals of the **Interoperability of Digital ID and Digital Wallets in West Balkans**.

6.2 Project Management and Development Methodology (section 1.2 of the assessment grid)

- The tenderer should outline their **project management approach**, including key **milestones** and **deadlines** for the project.
 - This should include detailed timelines for development, testing, deployment, and support phases.
 - The tenderer must define the **roles and responsibilities** of all involved parties, ensuring clarity in the project workflow.
- The contractor should also describe the **development methodology** to be used (e.g., **Agile**, **Waterfall**, or **Hybrid**).
 - For **Agile methodology**, this might involve defining **sprints**, **scrum teams**, and regular reviews.
 - For **Waterfall**, this would involve clear sequential stages from requirements gathering to deployment.
- The development methodology should be chosen based on its suitability for the project scope, team structure, and the level of flexibility required to adapt to changes during the project lifecycle.

6.3 Operational Plan/Personnel Assignment Plan (section 1.3 of the assessment grid)

- The contractor should develop a **detailed operational plan**, specifying:
 - **Personnel assignments**: Roles, responsibilities, and the expertise of key team members involved in the project.
 - **Timelines**: A timeline indicating when specific tasks, phases, and deliverables will be completed.
 - **Work steps**: Specific actions required for each phase, including analysis, design, development, testing, and deployment.
- This plan should ensure that all activities are efficiently coordinated and completed on schedule, with clear accountability for all involved.

6.4 Test and Documentation Concept (section 1.4 of the assessment grid)

- The tenderer must describe the **testing process** to be followed throughout the project. This should include:
 - **Unit testing, integration testing, user acceptance testing (UAT)**, and any other relevant forms of testing.
 - The testing process should ensure the solution meets all requirements and functions correctly in a real-world environment.
- The **documentation concept** should outline how the system documentation will be managed, including:
 - **Technical documentation**, such as system architecture, source code annotations, and configuration management.
 - **User documentation**, including user manuals, help guides, and any training materials.
 - The contractor should ensure compliance with **IT security standards** in documentation practices, and ensure that all documentation is clear, complete, and accessible.

6.5 Additional Requirements (section 2 of the assessment grid)

The tenderer should also address any additional technical or methodological requirements that are critical to the success of the project. These include:

- **Compliance with national and international standards** (e.g., eIDAS 2.0, interoperability, data protection, security, accessibility).
- **Sustainability** of the system and ongoing support requirements (by the respective government).
- **Scalability and flexibility** of the solution to accommodate future updates or integrations.
- **Risk management strategies** for mitigating potential delays or challenges in project execution.

7. Human Resource

The tenderer is required to propose personnel on the basis of relevant CVs for the positions (as experts) specified and described here in terms of the areas of responsibility and qualifications. **The requirements regarding the format and content of the CVs are set out in Section 12**

The qualifications set out below reflect the requirements for achieving the maximum number of points in the technical assessment.

‘One year of professional experience’ is understood to mean 12 cumulative expert months with at least 18 expert days per month, provided no diverging definition is specified for individual qualifications.

7.1 Expert 1: Team Leader/Project Manager (Section 3.1 of the assessment grid)

This position is a key expert.

Responsibilities of Expert 1:

The Team Leader / Project Manager will provide overall leadership, coordination, and strategic direction throughout the entire implementation of the project. The expert will be responsible for managing workplans, ensuring timely delivery of milestones across all three phases, facilitating communication among regional and national stakeholders, and overseeing reporting and quality assurance processes. The Team Leader will serve as the main interface between the contractor, GIZ, and key institutional partners across the WB6.

Qualifications of Expert 1:

Education/training (Section 3.1.1 of the assessment grid)	A bachelor's degree in information technology, Computer Science, Software Engineering, Public Administration (with experience in digital transformation/eGovernment), Industrial Engineering/Engineering Management, Electrical Engineering, Computer Engineering, or Telecommunications Engineering.
Language (Section 3.1.2 of the assessment grid)	Knowledge of English, C1 in the Common European Framework of Reference for Languages
General professional experience (Section 3.1.3 of the assessment grid)	7 years of professional experience in the in the management of complex software development projects.
Specific professional experience (Section 3.1.4 of the assessment grid)	5 years of professional experience in actively managing software development or digital service projects for the public sector in EU Member States or EU candidate/potential candidate countries 2 years of professional experience in the implementation of digital public services or e-Government solutions, including working with eIDAS 2.0
Leadership/management experience (Section 3.1.5 of the assessment grid)	5 years of leadership experience as a project team leader or manager in a company
Experience in the field of development cooperation (Section 3.1.6 of the assessment grid)	N/A

Other (Section 3.1.7 of the assessment grid)	2 years of experience with EU digital policy frameworks, including eIDAS 2.0, digital identity, interoperability, or Single Digital Gateway initiatives
--	---

7.2 Expert 2: Solution Architect (Section 3.2 of the assessment grid)

This position is a key expert.

Responsibilities of Expert 2:

The Solution Architect will be responsible for designing the high-level technical architecture of the prototype, ensuring that it is scalable, secure, and aligned with both national eGovernment platforms and EU-level interoperability standards. The architect will ensure compliance with eIDAS 2.0, support wallet integration where feasible, and define the interoperability model for both wallet-based and mutual recognition-based scenarios. The role involves coordinating with technical teams from participating WB6 economies to ensure architectural consistency and integration feasibility.

Qualifications of Expert 2:

Education/training (Section 3.2.1 of the assessment grid)	A bachelor's degree in information technology, Computer Science, Software Engineering, Electrical Engineering, Computer Engineering, or Telecommunications Engineering.
Language (Section 3.2.2 of the assessment grid)	Knowledge of English, C1 in the Common European Framework of Reference for Languages
General professional experience (Section 3.2.3 of the assessment grid)	10 years of professional experience actively designing and implementing software architecture, or large-scale digital system development
Specific professional experience (Section 3.2.4 of the assessment grid)	5 years of professional experience in actively developing design and architecture of eGovernment systems 3 years of professional experience in projects involving digital identity or digital wallets or trust services aligned with EU standards
Leadership/management experience (Section 3.2.5 of the assessment grid)	3 years of leadership experience as a technical lead, lead architect or solution designer in cross-functional or multi-country software teams
Experience in the field of development cooperation (Section 3.2.6 of the assessment grid):	N/A

Other (Section 3.2.7 of the assessment grid)	2 years of experience with EU digital policy frameworks, including eIDAS 2.0, digital identity, interoperability, or Single Digital Gateway initiatives
--	---

7.3 Expert 3: ICT Business Analyst (Section 3.3 of the assessment grid)

Responsibilities of Expert 3:

The ICT Business Analyst will be responsible for gathering, analysing, and validating business and functional requirements for the selected cross-border e-service prototype. Working closely with national stakeholders, the analyst will assess existing eGovernment services and digital wallet ecosystems across the WB6 economies, define user and system needs, and translate them into clear technical specifications for co-development. The role also includes supporting interoperability modelling, documenting service flows, and contributing to the design and validation of user journeys and use cases, ensuring alignment with EU digital policy frameworks and national priorities

Qualifications of Expert 3:

Education/training (Section 3.3.1 of the assessment grid)	A bachelor's degree in information technology, Business Informatics, Computer Science, Software Engineering, Electrical or Computer Engineering, Public Administration (only if combined with documented experience in digital transformation or eGovernment projects)
Language (Section 3.3.2 of the assessment grid)	Knowledge of English, C1 in the Common European Framework of Reference for Languages
General professional experience (Section 3.3.3 of the assessment grid)	6 years of professional experience in the area of requirements analysis or IT business analysis or system design in digital transformation projects
Specific professional experience (Section 3.3.4 of the assessment grid)	4 years of professional experience in analysing or specifying and documenting functional and non-functional requirements for eGovernment or public sector digital services 2 years of professional experience in cross-border or interoperability-related or digital identity projects in EU Member States or EU candidate/potential candidate countries
Leadership/management experience (Section 3.3.5 of the assessment grid)	N/A

Development cooperation experience (Section 3.3.6 of the assessment grid)	N/A
Other (Section 3.3.7 of the assessment grid)	2 years of experience with EU digital policy frameworks, including eIDAS 2.0, digital identity, interoperability or Single Digital Gateway initiatives

7.4 Expert 4: Technical Lead / Integration Engineer (Section 3.4 of the assessment grid)

Responsibilities of Expert 4

The Technical Lead / Integration Engineer will oversee the technical implementation of the prototype and ensure seamless integration with national eGovernment systems and digital wallet infrastructures. The expert will coordinate with national IT providers to implement interoperability models, align APIs, and manage the secure exchange of data and credentials. Responsibilities include leading technical troubleshooting, ensuring compliance with relevant standards (e.g., OAuth2, OpenID Connect, eDelivery), and supporting the refinement, testing, and validation of system components across the WB6. The role demands close collaboration with both local developers and institutional stakeholders to ensure successful integration and deployment

Qualifications of Expert 4:

Education/training (Section 3.4.1 of the assessment grid)	A bachelor's degree in information technology, Computer Science, Software Engineering, Computer Engineering, or Telecommunications Engineering.
Language (Section 3.4.2 of the assessment grid)	Knowledge of English, C1 in the Common European Framework of Reference for Languages
General professional experience (Section 3.4.3 of the assessment grid)	8 years of professional experience in the area of software development, systems integration, or IT infrastructure management
Specific professional experience (Section 3.4.4 of the assessment grid)	5 years of professional experience in designing or integrating or deploying complex information systems in the public sector 3 years of professional experience in interoperability or cross-border digital services projects involving API-based data exchange or authentication or digital wallet integration

Leadership/management experience (Section 3.4.5 of the assessment grid)	3 years of leadership experience as a technical team lead or senior developer or integration coordinator in software implementation projects
Development cooperation experience (Section 3.4.6 of the assessment grid)	N/A
Other (Section 3.4.7 of the assessment grid)	2 years of experience in secure system integration using standards such as OAuth2, OpenID Connect, SAML, or eDelivery

7.5 Expert 5: Data Protection & Compliance Expert (Section 3.5 of the assessment grid)

Responsibilities of Expert 5

The Data Protection and Compliance Expert will be responsible for ensuring that the prototype and all related processes comply with data protection legislation, cybersecurity regulations, and EU digital governance frameworks. This includes conducting risk assessments, advising on the implementation of safeguards for personal data and trust services, and supporting the development of privacy and security documentation. The expert will ensure alignment with the General Data Protection Regulation (GDPR), eIDAS 2.0, and relevant national laws, and contribute to institutional readiness through guidance, review, and awareness-raising activities across the WB6 economies

Qualifications of Expert 5:

Education/training (Section 3.5.1 of the assessment grid)	University degree or formal qualification in Law, Information Security or Data Protection (e.g. LLB, CIPP/E, CIPM, ISO/IEC 27001 Lead Implementer).
Language (Section 3.5.2 of the assessment grid)	Knowledge of English, C1 in the Common European Framework of Reference for Languages
General professional experience (Section 3.5.3 of the assessment grid)	8 years of professional experience in consulting projects with regards to data protection or information security or regulatory compliance (e.g. privacy law, cybersecurity governance, trust services)
Specific professional experience (Section 3.5.4 of the assessment grid)	5 years of professional experience in compliance advisory or privacy consulting for public sector digitalization projects 2 years of professional experience in cross-border or EU-regulated digital service environments, involving compliance with

	eIDAS or GDPR or other equivalent EU-level legal and technical standards
Leadership/management experience (Section 3.5.5 of the assessment grid)	N/A
Development cooperation experience (Section 3.5.6 of the assessment grid)	N/A
Other (Section 3.5.7 of the assessment grid)	2 years of experience in conducting compliance risk assessments or privacy impact assessments (PIAs) or implementing data protection measures in alignment with EU digital legislation

7.6 Expert 6: Legal / Trust Services Advisor (Section 3.6 of the assessment grid)

Responsibilities of Expert 6:

The Legal / Trust Services Advisor will provide expert guidance on legal, regulatory, and policy matters related to digital identity, qualified trust services, and cross-border interoperability. The expert will ensure alignment of the prototype and related processes with eIDAS 2.0, GDPR, and applicable national legislation. This expert will support the identification and mitigation of legal risks, contribute to the drafting of legal interoperability documentation (e.g. MoUs, agreements), and advise on recognition conditions for trust service providers across WB6 jurisdictions. The role includes close collaboration with national institutions, supervisory bodies, and technical teams to ensure the solution is legally compliant and scalable

Qualifications of Expert 6:

Education/training (Section 3.6.1 of the assessment grid)	A bachelor's degree in law with demonstrated specialization or certification in Digital Governance or ICT Law (e.g. EU Digital Law certificate).
Language (Section 3.6.2 of the assessment grid)	Knowledge of English, C1 in the Common European Framework of Reference for Languages
General professional experience (Section 3.6.3 of the assessment grid)	8 years of professional experience in the area of ICT law or regulatory compliance or legal advisory in digital transformation projects
Specific professional experience (Section 3.6.4 of the assessment grid)	5 years of professional experience in EU trust services or electronic identification, or digital public service legislation

	3 years of professional experience in cross-border recognition frameworks or qualified trust services or legal interoperability models
Leadership/management experience (Section 3.6.5 of the assessment grid)	N/A
Development cooperation experience (Section 3.6.6 of the assessment grid)	N/A
Other (Section 3.6.7 of the assessment grid)	2 years of experience in eIDAS 2.0 alignment or trust service accreditation or legal analysis for public sector IT solutions

7.7 Expert 7: UI/UX & Accessibility Specialist (Section 3.7 of the assessment grid)

Responsibilities of Expert 7:

The UI/UX & Accessibility Specialist will be responsible for designing intuitive, user-centred, and accessible interfaces for the cross-border e-service prototype. This includes ensuring compliance with recognized accessibility standards (e.g., WCAG), optimizing user journeys across multilingual and multi-jurisdictional contexts, and conducting usability testing with end users. The specialist will collaborate closely with technical teams and stakeholders to create inclusive digital experiences that meet the needs of diverse user groups across the WB6 economies

Qualifications of Expert 7:

Education/training (Section 3.7.1 of the assessment grid)	Bachelor's degree in UX Design, Human-Computer Interaction, Digital Media or Information Technology
Language (Section 3.7.2 of the assessment grid)	Knowledge of English, C1 in the Common European Framework of Reference for Languages
General professional experience (Section 3.7.3 of the assessment grid)	6 years of professional experience in the area of user interface/user experience (UI/UX) design or digital service design
Specific professional experience (Section 3.7.4 of the assessment grid)	3 years of professional experience in accessibility design and inclusive user interfaces 3 years of professional experience in eGovernment or public sector digital services

Leadership/management experience (Section 3.7.5 of the assessment grid)	N/A
Development cooperation experience (Section 3.7.6 of the assessment grid)	N/A
Other (Section 3.7.7 of the assessment grid)	2 years of experience in applying Web Content Accessibility Guidelines (WCAG) and designing multilingual or mobile-responsive or inclusive public interfaces

7.8 Expert 8: Training & Capacity Building Expert (Section 3.8 of the assessment grid)

Responsibilities of Expert 8:

The Training & Capacity Building Expert will design and deliver targeted training programs to enhance the skills of public officials, IT staff, and institutional stakeholders across the WB6. Responsibilities include developing workshop materials, facilitating in-person and virtual training sessions, supporting knowledge transfer on digital identity, interoperability, and trust services, and ensuring long-term institutional capacity for maintaining and scaling the prototype solution

Qualifications of Expert 8:

Education/training (Section 3.8.1 of the assessment grid)	Bachelor's degree in the area of Education, Public Administration, ICT or Human Resource Development
Language (Section 3.8.2 of the assessment grid)	Knowledge of English, C1 in the Common European Framework of Reference for Languages
General professional experience (Section 3.8.3 of the assessment grid)	7 years of professional experience in the area of training or curriculum development or organizational capacity development
Specific professional experience (Section 3.8.4 of the assessment grid)	5 years of professional experience in delivering capacity-building activities related to digital transformation or eGovernment 3 years of professional experience in working with public sector institutions in EU Member States or EU candidate/potential candidate countries
Leadership/management experience (Section 3.8.5 of the assessment grid)	N/A

Development cooperation experience (Section 3.8.6 of the assessment grid)	N/A
Other (Section 3.8.7 of the assessment grid)	2 years of experience in training of trainers (ToT) methodologies, adult learning, and evaluation of learning outcomes

7.9 Expert 9: DevOps / Cybersecurity Specialist (Section 3.9 of the assessment grid)

Responsibilities of Expert 9:

The DevOps / Cybersecurity Specialist will ensure the secure configuration, deployment, and performance of the prototype solution across test and live environments. Responsibilities include advising on infrastructure setup, implementing CI/CD pipelines, monitoring system performance, addressing vulnerabilities, and ensuring alignment with cybersecurity best practices and compliance frameworks such as eIDAS, GDPR, and ISO/IEC 27001. The expert will also support resilience, incident response planning, and secure data exchange protocols

Qualifications of Expert 9:

Education/training (Section 3.9.1 of the assessment grid)	Bachelor's degree in computer science, Cybersecurity, or IT Infrastructure, or a recognized certification such as CompTIA Security+, CISSP, or CEH
Language (Section 3.9.2 of the assessment grid)	Knowledge of English, C1 in the Common European Framework of Reference for Languages
General professional experience (Section 3.9.3 of the assessment grid)	8 years of professional experience in the area of IT infrastructure, cybersecurity, or DevOps engineering
Specific professional experience (Section 3.9.4 of the assessment grid)	4 years of professional experience in implementing secure software deployment pipelines (CI/CD) 3 years of professional experience in public sector or cross-border environments with regulatory constraints (e.g. GDPR, eIDAS)
Leadership/management experience (Section 3.9.5 of the assessment grid)	N/A
Development cooperation experience (Section 3.9.6 of the assessment grid)	N/A

Other (Section 3.9.7 of the assessment grid)	2 years of experience in implementing security-by-design principles, monitoring frameworks, and DevSecOps practices
--	---

The tenderer must assign all the proposed experts to the required qualifications and clearly present them in a separate table preceding the CVs. The summary presentation must mention only qualifications that are indicated in the CVs. Evidence of professional experience must be rendered in the form of meaningful references in the CVs. It is advisable to make specific reference to each instance of professional experience.

Soft skills of team members

In addition to their specialist qualifications, all team members are also expected to have the following qualifications:

- Team players
- Initiative
- Communication skills
- Sociocultural and intercultural skills
- Efficient partner- and client-oriented working methods
- Interdisciplinary thinking

Soft skills will not be evaluated.

8. Costing requirements

8.1 Assignment of experts

In your tender, please do not deviate from the specification of quantities required in these ToR. This is part of the competitive tender and is used to ensure that the tenders can be compared objectively. Please note only services that were commissioned by GIZ and rendered by the contractor will be remunerated. We would also like to point out that it may not be necessary to make use of the total number of proposed expert days.

The number of expert days corresponds to full working days.

Expert	Expert days
Expert 1: Team Leader / Project Manager	65
Expert 2: Solution Architect	50
Expert 3: ICT Business Analyst	45

Expert 4:	
Technical Lead / Integration Engineer	60
Expert 5:	
Data Protection & Compliance Expert	30
Expert 6:	
Legal / Trust Services Advisor	25
Expert 7:	
UI/UX & Accessibility Specialist	30
Expert 8:	
Training & Capacity Building Expert	25
Expert 9:	
DevOps / Cybersecurity Specialist	35
Total:	365

8.2 Travel expenses

8.2.1 Travel – sustainability considerations

GIZ would like to reduce greenhouse gas emissions (CO₂ emissions) caused by travel. When preparing your tender, please incorporate options for reducing emissions, for example by selecting the lowest-emission booking class (economy) or using means of transport, airlines and flight routes that are more CO₂-efficient. For short distances, travel by train (second class) or e-mobility are the preferred options.

CO₂ emissions resulting from air travel must be offset. GIZ specifies a budget for this which enables carbon offsets can be settled against evidence.

There are many different providers in the market for emissions certificates, and they have different climate impact ambitions. The [Development and Climate Alliance](#) has published a [list of standards](#) (only in German available). GIZ recommends using the standards specified there.

8.2.2 Travel expense requirements

Travel expense budget: EUR 41,500.00

Budget for CO₂ offsets for flights: EUR 700.00

An unalterable budget for CO₂ offsets for settlement against evidence is specified.

As the number and duration of the business trips is not yet clear, the above-mentioned unalterable travel expense budget for all trips in Germany and abroad for experts is specified in the price schedule. The budget contains the following travel expenses:

- Per-diem allowances and accommodation allowances
- Flights and other transport costs
- Ancillary travel expenses (visa, etc.)

The costs are reimbursed as a lump sum (per-diem allowances up to the maximum amounts permissible under tax law for each country) as set out in the country table in the circular from the German Federal Ministry of Finance on the reimbursement of travel expenses (see <https://www.bundesfinanzministerium.de>), or on presentation of evidence (airfares and other main transport costs).

Notes on the settlement of accommodation allowances outside:

For the country Albania, Bosnia and Herzegovina, Kosovo, North Macedonia, Montenegro, and Serbia, tenderers may offer accommodation allowances up to EUR 116.00 in Albania, EUR 109.00 for Bosnia and Herzegovina, EUR 71.00 for Kosovo, EUR 89.00 for North Macedonia, EUR 85.00 for Montenegro, EUR 97.00 for Serbia. This is the maximum amount permissible under tax law as per the BMF circular on travel expense reimbursement. The **evidenced expenses** will be reimbursed up to the contractually agreed amount.

All travel activities must be agreed in advance with the project manager. Travel expenses must be kept as low as possible.

Please note: These travel expense items do not cover costs related to the contract in the country of assignment (see section 3.6.2 of the General Terms and Conditions). Please cost these items if applicable in the price schedule under '2.2 Costs related to the contract in the country of assignment'.

8.3 Workshops, training

– not applicable –

8.4 Flexible remuneration

Budget for flexible remuneration: EUR 20,000.00

The fixed, unalterable budget above is given in the price schedule for flexible remuneration. Flexible remuneration is intended to facilitate the flexible management of the contract by the officer responsible for the commission at GIZ. The contractor can make use of the funds in accordance with Section 21.5 of the GIZ's Special Terms and Conditions of Contract.

9. Requirements on the format of the tender

The structure of the tender must correspond to the structure of the ToR. It must be legible (font size 11 or larger) and clearly formulated. The technical bid must be submitted in English

The technical and methodological concept of the tender (Section 6 of the ToR) is not to exceed 20 pages (not including the cover page, list of abbreviations, table of contents and

Transaction number: 81322924

brief introduction). Additional annexes not requested will not be assessed. External content (e.g. links to websites) will also not be considered.

The CVs of the staff proposed in accordance with Section 7 of the ToR must be in the EU format and not more than 4 pages in length. The CVs must clearly show what position the proposed person held, which tasks they performed and how many expert days they worked during which period in the specified references.

We strongly request that you do not exceed the number of pages specified.

The CVs must clearly and unequivocally show what position the proposed person held, which tasks they performed and how long they worked during which period in the specified references. **The references contained in the CVs must therefore include the following information:**

- Name of the company/organisation/reference project in which the expert worked
- Position held and task(s) performed by the expert in the company/organisation/reference project
- Work outcomes or products produced by the expert, or expert's contribution to the completion of these outcomes and projects (if relevant)
- Duration of the expert's assignment in the company/organisation/reference project per calendar year in full-time expert days, weeks or months (for example: 2019: 2 months, 2020: 10 months, 2021: 1 month)
- Leadership experience/management: clear information on the reference projects or fixed positions within the company/organisation in which the requirements specified in Section 7 were fulfilled (for example, period, number of persons for whom the expert had disciplinary responsibility, project budget) (if relevant)
- International professional experience/professional experience in the country of assignment: clear information on the reference projects or fixed positions in the company/organisation in which the requirements specified in Section 7 were fulfilled (for example, actual duration of assignment on the ground in full-time expert days, weeks or months) (if relevant)

In order to facilitate the assessment, we request that you number the references consecutively and provide only references that are clearly related to the object of this tender.