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

Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Project title:

IKI Indonesia Website Development and Maintenance

From June 2024 – December 2025

Country:

Indonesia

Subject of the tender procedure:

Open Tender

Processing number/ cost centre:

20.9041.3-002.00

Transaction number:

0. List of abbreviations 3

1. Context 4
1.1 The company 4
1.2 Project background 4
1.3 Objective of the procurement 5

2. Requirements for the IT solution 5
2.1 Description of the existing IT solution 5
2.2 Description of the application/use of the IT solution 6
2.3 General conditions at the partner end 6
2.4 Functional requirements 6
2.5 Non-functional requirements 8
2.5.1 Interfaces 8
2.5.2 System requirements/technical framework 9
2.7 Hosting 9

3. Responsibilities of the contractor 9
3.1 Work package 1: *Kick-off* 9
3.2 Work package 2: *Developing visual design, website menu, landing page and other content for website.* 10
3.3 Work package 3: *Digital Accessibility and Testing* 10
3.4 Work package 4: *Final deployment* 10
3.5 Work package 5: *Training* 10
3.6 Work package 6: *Regular Maintenance* 10

4. Schedule and milestones 10

5. Data protection and information security 11

6. Technical-methodological concept 14
6.1 **Requirements for the technical-methodological concept (section 1 of the assessment grid)** 14
8.1.1 Assessment of the requirements: 14
8.1.2 Project management and development methodology: 14
8.1.3 Operational plan/personnel assignment plan: 14
8.1.4 Test and documentation concept: 14
6.2 Additional requirements (section 2 of the assessment grid) 14

7. Human resources 15
7.1 Human resources concept 15

8. Costing requirements 16
8.1 Website development and maintenance 16
8.2 Workshops, training 16
8.3 Hosting 16
8.4 Other costs 16
8.5 Flexible remuneration item 16

9. Requirements on the format of the tender 16

10. Sustainability Planning (Hand-over) 17

11. Annex 1 17

0. List of abbreviations

BMWK	**Supplementary Terms and Conditions for the Procurement of IT Services**

1. Context

1.1 The company

Supported by German Federal Ministry for Economic Affairs and Climate Action (BMWK) through the International Climate Initiative (IKI), Climate and Biodiversity Hub Indonesia (Bappenas's component) supports Bappenas in mainstreaming its climate and biodiversity policies into national development planning. To this end, it trains staff of relevant line ministries and strengthens cooperation with civil society and academia. The project also advises on improving competencies for transparent reporting, financial resource mobilization and knowledge exchange with the international community.

This project also has a special performs the interface project function to connect all IKI implementing partners and create an opportunity to exchange lesson learned, experience, and knowledge through series of activities and product knowledge e.g., IKI networking workshop, special/thematic topic discussion, and IKI newsletter.

The Governments of Germany through Federal Ministry for Economic Affairs and Climate Action (BMWK) in close cooperation with the Federal Ministry for the Environment, Nature Conservation, Nuclear Safety and Consumer Protection (BMUV) and the Federal Foreign Office (AA) together with the national and sub-national government of Indonesia.

Indonesia, as one of 14 IKI priorities countries hosts up to **49 IKI projects** consists of 12 bilateral, 11 regional, and 26 global projects (data per December 2023). During this 2023, the IKI Hub has organized one technical & high-level delegation visit to Berlin, two thematic workshops on biodiversity and energy, and one networking workshop on the interlinkages between climate, biodiversity, and energy. In addition, 2023 also marks an important milestone of IKI Digital Transformation plan because the IKI Newsletter format has changed from an old version in PDF to digital version (MailingWork email format).

1.2 Project background

Since 2023, the IKI Hub Indonesia has implemented the digital transformation plan that consists of transforming IKI Indonesia Newsletter from PDF format to digital, Communication and Digital Training, until the development of IKI Indonesia website

From June-July 2023, the IKI Hub shared the survey questioning input/views from IKI projects related to the digital transformation including the website development. See below some relevant findings:

- From 17 out 20 responders supported the idea of IKI Indonesia website development.
- Some reasons have been mentioned by responders such as
  - Good to have "digital interface" to introduce what is IKI and its contributions in Indonesia.
  - Vital platform for outreach/exchange of IKI Indonesia
  - Promote the visibility of IKI projects in Indonesia and provide wider accessibility for wider public.
  - Help to identify potential collaborations.

- During steering committee (SC) team with Ministry of National Development Planning in Indonesia in July, there is a statement and request from Director of Environment who expect the IKI Hub Indonesia to develop its website.

Responding to that, then in this 2024, the IKI Hub is planning to develop the IKI Indonesia website that aims at building brand presence of IKI in Indonesia, showcase expertise and portfolio of IKI projects, and connect the website with IKI Indonesia newsletter. This is also in line with a request by Ministry of Ministry of National Development Planning (Bappenas) who expects the IKI Indonesia website to serve as repository of Bappenas' efforts towards the work of climate and biodiversity in collaboration with IKI projects in Indonesia.

To support the IKI Hub team to develop a website and implement the maintenance, a website developer company/consultant will be hired.

1.3 Objective of the procurement

The website developer is expected to provide following services:

- To develop a visual design of IKI Indonesia website by integrating the IKI grand design and colour palette with a little touch of Indonesia arts/icons.
- To develop a website based on the required website menu provided by GIZ.
- To create both website format in desktop and mobile version.
- To manage the server of website by ensuring the security and data protection standards required by GIZ.
- To provide strategic inputs and feedback during the website development phase to GIZ.
- To manage the website domain of IKI Indonesia website.
- To ensure that smooth and fast access of website as well as comply with digital accessibility standards of Web Content Accessibility Guidelines (WCAG).
- To implement the website maintenance including dealing with possible errors, attacks, hacks from the development until implementation.

2. Requirements for the IT solution

2.1 Description of the existing IT solution

The IKI Hub Indonesia hasn't have any website at the moment. The information and/or content about IKI projects in Indonesia are shown generally in IKI global website. There are some other IKI interface projects who already have their own website, such as IKI India, IKI Peru, and IKI Mexico.

The IT solution that IKI Hub Indonesia utilises is the MailingWorks – an official and legitimate newsletter platform from GIZ to develop and publish digital newsletter and manage subscription.

With this background, the development of IKI Indonesia website will start from stretch by incorporating inspiration and idea from IKI global website and other IKI interface project websites.

2.2 Description of the application/use of the IT solution

With the absence of IKI Indonesia website, we deem this is important to develop the website and to synchronize it with IKI Indonesia newsletter and general information shown on the IKI global website.

By having the IKI Indonesia website, it will increase the brand presence of IKI support in Indonesia, provide a uniform platform to show IKI project's portfolio and contribution to Indonesia's climate and biodiversity, as well as, to connect current IKI newsletter to website.

Some targeted audiences are identified ranging from IKI implementing projects and consortium partners in Indonesia, Indonesian and Germany government, Indonesian research and academy institution, as well as wider public who has interest and passion on climate, biodiversity, and other environmental issues.

With the current digital age in Indonesia, it is expected that IKI Indonesia website will be available on desktop and mobile format and accessible to people with disability.

2.3 General conditions at the partner end

- The website developer is a company not individual consultant and has Indonesian legal identity and document.
- Preferred developer has their own/in-house UI/UX designer, system developer, and other relevant roles to support the project.
- Have competency and experience in developing website for non-profit/international organisation.
- Able to host a server, manage, and secure the website domain.
- Have experience on website/digital accessibility.

2.4 Functional requirements

There are some functional requirements for this website development such as:

a) The website shall be implemented in one language which is English.

b) The design and content should be accessible through desktop and mobile including for people with disability.

c) The location of server is preferably in Indonesia or country nearby to Indonesia. The website management will be managed by the IKI Hub Indonesia as part of mandated assignment as the IKI interface project. The future management of the website will be continuously managed by GIZ project who owns the mandate as IKI interface project in Indonesia and/or Ministry of National Development Planning (Bappenas).

d) The preferred system is blog/web press that represents the IKI global design and current trend.

e) Extensive knowledge on SEO and back-link will be desirable.

f) The planned website menu:

1. **Home**
   To return to main landing page

2. **About Us**
   About IKI in Indonesia
   Statistics of current IKI project in Indonesia

3. **Projects**
   Based on 4 IKI funding areas: MITIGATION, ADAPTATION, FORESTRY/REDD+, BIODIVERSITY

   Under each area, there will be a list of ongoing and finished projects.

4. **What's New**
   - IKI News
   - Project News
   - Human Impact Stories
   - Gender Updates
   - Knowledge Product

   Containing any knowledge product published by IKI projects in Indonesia.

5. **Upcoming Events**
   Upcoming Events

6. **Gallery**
   Photo and video documentation of IKI Hub Indonesia activities (or IKI implementing projects)

7. **Contact us**
   It contains address and email IKI Hub Indonesia.

g) The planned landing page:

The landing page is expected to be highly interactive and tech sophisticated in generating/providing the data, information, and highlight in visually pleasant manners. The use of AI is welcome to provide user with new experience in getting to know about IKI works in Indonesia.

1. **Header area**
   - Branding: BMWK – IKI Indonesia – GIZ
   - Accessibility Information
   - Disclaimer and Data Privacy Policy
   - Search

2. **Interactive landing page menu**
    - Photo banner slice (1-5 photos) taken from Project News, Gender, Human Impact Stories, IKI News
    - Short information about IKI Hub Indonesia
    - Statistics of active/ongoing IKI projects in Indonesia
    - Location mapping of IKI project in Indonesia
    - Testimony of completed IKI projects
    - Upcoming Events

3. **Footer**
    - Newsletter Subscription
    - Contact Us

Imprint and privacy policy

Any content published on behalf of IKI implementing projects and consortium partners shall reflect the owner of content through writer information and content tagging.

The website developer shall provide a disclaimer format below:

- The information, data, and views in this content and website are the opinions/views of the authors and do not represent the position of the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH, The German Federal Ministry for Economic Affairs and Climate Action (BMWK), and the International Climate Initiative (IKI).

Along with this data privacy policy:

- Our server collects information from visitors' web browser, operating system, and web address that generate links to our website. The general information will only be used to analyse the website performance and improve the functionality if necessary and will not be used for other purposes and transferred to third parties.

2.5 Non-functional requirements

The following non-functional requirements must be taken into account by the contractor when implementing the service.

2.5.1 Interfaces

This website will not collect any personal information. The data and information shown on this website will be taken from IKI Indonesia newsletter and other sources provided by IKI projects.

The type of data and information shown will be content article, video, infographic, published research and other external knowledge product made by IKI implementing projects and consortium partners in Indonesia.

2.5.2 System requirements/technical framework

The IKI Indonesia website shall be accessible according to following points:

- **Operational Systems**
  Mac OS X v10.4 Tiger and later
  Windows 7 and later

- **Browser both on Desktop and Mobile**
  Google Chrome version 49 and later
  Microsoft Edge version 15.150063 and later
  Safari version 10 and later
  Mozilla Firefox version 54 and later
  Xi or Xiaomi browser

- **Digital accessibility**
  The website (design, colour contract, navigation) and its content (alternative text, colour contrast, closed caption on video, font and font size) are digitally accessible according to Web Content Accessibility Guideline (WCAG)

- **Website Security**
  The website development shall implement one or more standard of protecting website from potential attacks and hacks. One of them is by utilizing the Open Web Application Security (OWASP).

2.7 Hosting

The website developer is responsible to manage the domain and hosting for this IKI Indonesia website. The domain name will be decided later on once the website developer is appointed.

The desired hosting for this service is managed server, located in Indonesia or neighbouring countries like Singapore/Australia. For initial stage, the desired CPU is Cores 8 or later with RAM 8192 MB, capacity 160 GB, and bandwidth unmetered.

The appointed website developer is free to provide other options for managed server/hosting as long as it meets the standard of security.

Please note: Before commissioning or at the latest before going live, the data collection and processing of the developed application as well as the server must be individually checked with the GIZ data protection management.

3. Responsibilities of the contractor

The contractor must 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:

3.1 Work package 1: *Kick-off*

Services to be provided by the contractor:

- Documentation of the agreements
- Establishment working timeline.
- Decision on website design and navigation.
- Decision on website name (domain) and its hosting.

3.2 Work package 2: *Developing visual design, website menu, landing page and other content for website.*

- Translating the idea from work package 1 into the design, computer programme, and coding.
- Setting up the domain and hosting server.
- Incorporating some dummy content for each website menu.
- Designing landing page based on above required content.

3.3 Work package 3: *Digital Accessibility and Testing*

- Integrating some digital accessibility guidelines into the website
- Testing the website's performance and its accessibility through desktop and mobile phone.
- Documentation of user feedback and experience and plan for improvement.

3.4 Work package 4: *Final deployment*

- Final deployment to the real website from the dummy page.
- Solving the bugs/glitch after the deployment.
- Facilitating final inputs and revision after deployment.

3.5 Work package 5: *Training*

- Creating a manual book on CMS of website.
- Delivering the training to appointed administrators of website.
- Assisting administrators in case by case basis if needed.

3.6 Work package 6: *Regular Maintenance*

- Maintaining daily back up of website.
- Bug, error, and glitch fixing.
- Protecting the website from attacks/hacks and reporting the incident to GIZ.
- Providing monthly analytics reports.
- Monitoring the domain and hosting server.

  and other relevant duties.

4. Schedule and milestones

Period of Agreement: **June 2024 – December 2025 (18 months)**

Milestones	Delivery date/period
Milestone 1 – Kick off	End of June 2024

Domain name, hosting, and visual design for website (15%)	
Milestone 2 – Design and website development (40%)	End of September 2024
Milestone 3 – Final deployment and training (15%)	End of December 2024
Milestone 4 – Website maintenance (30%)	January – December 2025

5. Data protection and information security

The provisions on data protection and information security of the current version of GIZ's General Terms and Conditions of Contract (section 1.10 Data protection) apply.

Data protection in general

Personal data will be processed on behalf of the client. Therefore, an agreement on "Outsourcing of data processing (AuV)" will be concluded with the contractor in accordance with Art. 28 GDPR. For this purpose, the technical and organisational measures (TOM) for compliance with the data protection requirements must be outlined prior to conclusion of the contract. If the contractor has already been audited by GIZ in the past, an update in accordance with GDPR must nevertheless be sent. After a positive check, the contract is concluded with the AuV attachment.

Data protection by design and by default

The digital tool developed, upgraded or used on behalf of GIZ must meet the highest data protection standards, especially the GDPR's data protection by design and by default requirement, as elaborated in Annex 1. The development of a data processing system under the GDPR, to offer practical orientation to the contractor."

Information security

The following points must be considered by the contractor and if they are not within the contractor's responsibility or scope of work, they must at least be discussed with the partner's project team in order to close any existing security gaps.

The contractor must inform the client immediately and in an appropriate form about security incidents that may affect the client. If the contractor has appointed an IT security officer or another person to receive such information, the information must be sent directly to this person.

The contractor is obliged to make the client's data available at the end of the contract without additional remuneration (for example, by providing the possibility of downloading).

At the end of the contract, the contractor shall immediately and without being requested to do so return all documents, auxiliary means, materials or objects received from the client which were not permanently left to the contractor for the purpose of executing the contract as intended. This shall also apply to all copies. Furthermore, all performance results in any form shall be handed over to the client; insofar as the granting of exclusive rights has been agreed, this shall apply including the copies made.

The contractor shall be permitted to demand secure deletion (i.e. non-reconstructible) or destruction in whole or in part instead of surrender. This shall be proven to the client upon request and at its discretion by means of a corresponding declaration or otherwise.

The following points in particular must be taken into account by the contractor for the operation and maintenance of websites.

- The hoster's data center(s) must be certified to ISO 27001 or the contractor must work according to the international standards of information security to ISO 27001 to ensure the highest standards of development and operation. If possible, refrain from using shared web servers or better provide our own virtual server for the project.
- A firewall must be installed upstream of the server (e.g., authorized IP addresses/GEO blocking or address ranges for logging on to the system can be entered here or also excluded for this purpose). Up-to-date anti-virus software must be used on the server and configured accordingly for automatic updates.
- Separate environments for development, testing and production must be provided.
- Network communication between the components of the application should be encrypted. Hard-coded keys (symmetric/asymmetric) should not be included in the application. If this is unavoidable, the handling of the key must be described. The information security risks related to the storage of the key must be evaluated. The transmission of authentication information (especially passwords) must be encrypted. The storage and transmission of sensitive and/or personal data must comply with current encryption standards.
- Separation of application and data is to be provided, i.e. an application server and a separate server for the database and file storage is provided, with communication through a firewall.
- A role and authorization concept must be implemented that includes at least the roles of system admin (full authorization to the entire system), CMS admin (+account management), editor and author (editing content/articles). The application to be developed must be operable with minimal system rights. Only the following user groups may have access to the backend: Developers and administrators of the Contractor as well as employees for editorial maintenance of the Contractor. Access to the backend at the operating system level may therefore only be granted to very limited user groups with the appropriate expertise. There must be a documented authorization concept for each application (e.g. in the operating manual).

- A password policy must be implemented, which should look like this:
  - minimum number of digits e.g. 12
  - latin capital letters (A-Z)
  - lower case Latin letters (a-z)
  - basic digits (0-9)
  - non-alphanumeric characters (like !, $, #, -, &)
  - your password must not contain the whole or parts of your login name!
  - after 5 wrong entries the account should be locked for 3 minutes
  - max. password age 90 days
  - password history, at least 5 different passwords in before a previously used password is accepted again, new passwords that differ only by consecutive numbers should not be accepted.

  Passwords must not be stored in plain text. Passwords may only be stored as hash values. The hash algorithm must conform to the current recommendations of the BSI (technical guidelines). Hard-coded passwords must not be included in the application. The transmission of authentication information (especially

passwords) must be encrypted. Changes to account data that are required for registration may only be made by the administrators and are to be blocked for the user.

- 2-factor authentication should be implemented for sensitive data or administrative accounts; Google Authenticator is not to be used for this. 2FA is to be possible via multiple channels (app, SMS or e-mail).
- When configuring the web server, you must pay attention to the following
    - Disable Trace HTTP Request
    - Run as a separate User & Group
    - Disable signature
    - Disable banner
    - Restrict access to a specific network or IP
    - Use only TLS 1.2
    - Disable Directory Listing
    - Remove unnecessary DSO modules
    - Disable Null and Weak Ciphers
    - periodically updates of the system -> stay current!
    - periodically checks of the system log files
- The system must be hardened against SQL injection. In detail, this concerns the validation, filtering and cleansing of user input. The inputs may only have expected properties and characters and may not contain any unauthorized metacharacters that are passed to the SQL interpreter.
- When implementing API interfaces, it is essential to harden them against malicious code injection (SQL injection, etc.) via the URL.
- The system must be protected against Cross Site Scripting (XXS) on the client side. The server(s) must be protected against reflected or persistent cross site scripting by securing the server source code. All data to be processed by the server must be validated before execution. Whitelists of permitted data can be used for this purpose. General conversion of certain script characters is also a popular method. It is to be prevented that executable metacharacters of the scripts are read by the server. Cookies should only be read by the server (HttpOnly) and not by JavaScript in the browser.
- For the upload of files, appropriate file filters are to be provided so that no files with executable content (scripts, programs or SQL codes) can be uploaded and executed.
- A system log is to be implemented in which at least logins and logouts of all users and actions such as updates, backups, uploads and downloads, changes to account data and authorizations, as well as all security-relevant actions and events are to be logged and documented. The inclusion of further log data is still to be discussed in detail with the project. The system log is to be documented in the operating manual.
- The error messages generated by the application (especially exception handling/exceptions) must not provide any information that allows conclusions to be drawn about the architecture or software/software versions used.
- The regular backups of the complete system are to be carried out by the Contractor and checked accordingly for usability (restore). The backup can be stored on the server, but a copy must always be stored offline to prevent loss through hacker attacks. The intervals for the backups are to be coordinated with the project. Important backups always belong offline on another system and must be validated
- The deletion procedure must be proven upon request. Legal retention obligations remain unaffected.
- Session cookies used for logins must be deleted after logging out from the client.

- In order to minimize operating errors (human errors), the ergonomics of the application should be designed safely according to the need for protection.

6. Technical-methodological concept

In the conceptual design of the tender (technical-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 **Requirements for the technical-methodological concept (section 1 of the assessment grid)**In the tender, the tenderer is required to show *how* the services specified in section 3, where relevant taking account of other specific methodological requirements (section 2), are to be provided (technical-methodological concept).

8.1.1 Assessment of the requirements:

The tenderer must assess the objective and the requirements of the IT solution (see sections 1 and 2) in relation to feasibility and to what particular (non-)technical difficulties must be taken into account in the IT solution to be developed by the tenderer in regard to the objective (section 1.1 of the assessment grid).

8.1.2 Project management and development methodology:

The tenderer should consider the design of the project management process and describe his or her methodology for development/implementation, taking into account the described work packages (section 3) and compliance with the milestones (section 4) (section 1.2 of the assessment grid).

8.1.3 Operational plan/personnel assignment plan:

The tenderer must create and explain an operational plan that also includes a personnel assignment plan for all of the specialist staff that he or she offers. The operational plan must depict the assignment periods (time period and expert days) and, in particular, describe the necessary work steps and take account of and, where necessary, supplement the milestones as per section 4 (section 1.3 of the assessment grid).

8.1.4 Test and documentation concept:

The tenderer must describe the process for testing and documenting the IT solution and the IT security and documentation standards used (section 1.4 of the assessment grid).

6.2 **Additional requirements (section 2 of the assessment grid)**

The tenderer should submit the offered design of landing page according to the desirable design mentioned on the brief.

7. Human resources

7.1 Human resources concept

The tenderer is required to provide staff for the positions ('experts') referred to and described here in terms of the scope of tasks and qualifications on the basis of corresponding CVs (see section 7).

requirements for achieving the highest score in the technical assessment.

Expert 1: Team Leader (Section 3.1 of the assessment grid)

Qualifications:

- Education/training (3.1.1):
  University qualification (bachelor/master degree) in IT, computer science, website programme, UI/UX, Digital Marketing, or relevant field / proven to relate with the work.

- Language (3.1.2):
  Business fluency in English and Bahasa Indonesia

- General professional experience (3.1.3):
  5-7 years of professional experience in the computer science/website programme and other relevant experience.

- Specific professional experience (3.1.4):
  5 years of professional experience in computer science/IT/related topics

- Leadership experience/management (3.1.5):
  5-7 years of management/leadership experience as project team leader or manager in a company/a project related to IT application e.g. website, mobile application, etc.

- Development cooperation (DC) experience (3.1.6):
  2-3 years of experience in DC projects

Expert pool 1 'Project Manager'
Qualifications:

- Education/training (3.1.1):
  University qualification (bachelor/master degree) in IT, computer science, website programme, UI/UX, Digital Marketing, or relevant field / proven to relate with the work.

- Language (3.1.2):
  Business fluency in English and Bahasa Indonesia

- General professional experience (3.1.3):
  5-7 years of professional experience in the computer science/website programme and other relevant experience.

- Specific professional experience (3.1.4):
  6 years of professional experience in computer science/IT/related topics

- Leadership experience/management (3.1.5):
  5-7 years of management/leadership experience as project team leader or manager in a company/a project related to IT application e.g. website, mobile application, etc.

- Development cooperation (DC) experience (3.1.6):
  2-3 years of experience in DC projects

8. Costing requirements

8.1 Website development and maintenance

Budget for website development (including hosting, server, domain, design, etc.) and website maintenance is: EUR 15,789 from June 2024 – December 2025.

8.2 Workshops, training

The contractor is not responsible for the logistical organisation of the workshops and therefore the costs do not need to be specified.

The training delivery from contractor side will be included to costing point 8.1.

8.3 Hosting

Included to costing point 8.1.

8.4 Other costs

Included to costing point 8.1.

8.5 Flexible remuneration item

Budget for flexible remuneration: EUR 2500

The fixed, unalterable budget stated above for flexible remuneration is earmarked in the price schedule. 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 5.18 of the General 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 language in which the tender must be written is English.

The technical-methodological concept of the tender (section 7 of the ToR) is not to exceed 10 pages. The tenderer is allowed to submit their company profile and portfolio with max. 10 pages presented in different document than the technical-methodological concept.

The CVs of required personnel which are Team Leader and Project Manager must clearly show what position the proposed person held, which tasks he or she performed and how

many expert days he or she worked during which period in the specified references. The CVs should be submitted in English too.

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

10. Sustainability Planning (Hand-over)

Climate and Biodiversity Hub Indonesia performs special mandate as IKI interface project called 'IKI Hub' since 2022. This will project will continue the activities until April 2026.

The website management after final deployment will be managed by the Climate and Biodiversity Hub Indonesia. The future management of the website will be continuously managed by GIZ project who owns the mandate as IKI interface project in Indonesia in close coordination with Ministry of National Development Planning of Indonesia (Bappenas) as main political party.

11. Annex

1. The development of a data processing system under the GDPR
2. **Outsourcing of data processing - AuV (<u>Appendix II & III need to be filled out by bidder</u>)**