giz

ANNEX II.

TECHNICAL REQUIREMENTS TO DATA PROTECTION AND INFORMATION SECURITY

A. Data Protection

1. When processing personal data, the contractor and partner shall act as independent data controllers and must comply with all applicable data protection obligations, specifically law Nº 058/2021 of 13/10/2021 (Data Protection Act of Rwanda). They shall process personal data only when the given purpose cannot be reasonably attained without such data. Data protection principles such as lawfulness, data minimization, accuracy, purpose limitation, storage limitation, transparency, integrity and confidentiality, and accountability must be paid due attention to. In particular, the privacy law requires that the controller facilitates the exercise of the data subject's rights. The system must foresee and provide the possibility for the exercise of the following rights: the rights to rectification; erasure; and data portability; the right to withdraw consent; rights to restrict or object to processing (with these last two requiring the temporal deactivation of the profile without deleting any personal data). The GIZ is NOT in any way responsible for such processing.

2. Data protection by design and by default. The digital tool developed or updated/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 II.** *"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.*

3. GIZ shall be notified by the Service Provider if a new feature requested by the partner is not compliant with the privacy by design principle.

4. The current contract grants GIZ the right to audit or request a third-party audit of the Service Provider regarding the fulfilment of the security requirements as defined in the terms. Access to or processing of personal data will be excluded from the audit.

B. Information security

The following information security regulations apply to the service delivery

Handling confidential data

Any and all data relating to the contract and subsequent commissioning as well as any other information, such as submitted documents and exchanged information, of which the contractor and its employees become aware in the course of performing the contract, shall

be treated as confidential during and beyond the term of the contract. Furthermore, the need-to-know principle applies, i.e. such documents and information may be disclosed and made accessible only to persons to whom this information is absolutely essential for fulfilling their duties. This provision applies even if such documentation and information has not been explicitly designated as secret or confidential. The contractor is also not permitted to use this data and information for its own purposes.

Access to information

As previously stated, *the fulfilment of the contract does not involve access to live systems and do not entail any tasks that could be interpreted as data processing of personally identifiable production data.* Nevertheless, the following provisions apply to minimize unauthorized access:

- The service provider shall request access only to what is strictly necessary. Access shall be limited to the type of data based on the job role.

- Unless justified, the service provider shall prevent one staff from having end-to-end access to the ecosystem.

- Access of the service provider shall be time-bound. Consequently, access shall be automatically revoked when contract ends.

- The service provider shall regularly review and re-certify user access rights of the staff involved in this contract.

- User accounts must be tied to individual and shall not be shared among staffs of the service provider.

Retaining GIZ-related records, contract termination

Upon termination of the contract, the contractor shall return any other records, aids, materials and objects, which were passed to the contractor by *GIZ/MINALOC* on a non-permanent basis as intended, without delay and without being prompted to do so. This provision shall also apply to any copies of such items.

In the above-mentioned cases, the return shall follow a deletion procedure. GIZ is also entitled to request secure (i.e. not re-constructible) erasure or destruction, either in whole or in part. Evidence of the erasure and the erasing procedure used shall be provided to *GIZ/MINALOC* upon request, e.g. in a written declaration. There shall be no additional remuneration.

Statutory retention obligations and periods shall remain unaffected by this provision.

giz

Reporting security incidents

An information security incident is an event that may have – or already has – negatively impacted information security, for example through unauthorised viewing/disclosure of information (loss of confidentiality), modification of information (loss of integrity) or deletion of information/disruption of access to information (loss of availability).

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

The contractor shall inform GIZ (informationsecuritymanagement@giz.de) without delay and in an appropriate form about information security incidents which (also) affect GIZ information.

Use of devices and networks

When devices are used in the course of performing the contract, the contractor shall ensure that the place of use is properly secured and that unauthorised third parties cannot use them. Measures shall also be taken to ensure that unauthorised third parties cannot see any *GIZ/MINALOC*-related information (e.g. by applying privacy filters).

- Devices used by the service provider shall enforce following security requirements:
    - Web Filtering to block access to known phishing website
    - Multi-factor authentication (MFA) to protect account if credentials are stolen
    - End-Protection to block malware from phishing attachments
    - Limit what sensitive data can be shared via email
    - Track and analyse failed login attempts or unusual activity
    - Regular password change

- The service provider shall ensure that employed staffs are regular trained to spot phishing emails, report suspicious links and social engineering tactics.

- 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.

- 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

giz

Software development

The software to be developed and the development process shall satisfy the following requirements:

- Information security shall be the top priority for both the architecture and the functionality of the application (‘security by design’, ‘information security through technology design’).
- All IT systems and applications involved in software development shall be hardened in a suitable manner.
- The application to be developed shall be operable with minimum system rights.
- Network communication between the components of the application should be encrypted.
- Transmission of authentication information (particularly passwords) shall be encrypted.
- The application may not contain hard-coded passwords.
- The application should not contain hard-coded keys (symmetric/asymmetric). If this is unavoidable, the procedures for handling the key shall be described. The information security risks associated with storing the key shall be assessed.
- The application should be designed so that it can be tested and easily maintained (e.g. vulnerabilities can be remedied easily).
- To minimise incorrect use (human error), the application should be ergonomically designed to be secure and appropriate to the required level of protection.
- Entries made by users, data streams and secondary data (e.g. session information) shall always be validated, i.e. the application may not accept impermissible entries. Validation shall be performed in such a way that it cannot be circumvented (e.g. by manipulated client software).
- The error messages generated by the application (especially exceptions) may not provide any information that allows conclusions to be drawn about the architecture or the software/versions used.
- Users may not access application functionality or processed information until they have been authenticated/authorised.
- A documented permission concept is required for each application (e.g. in the operating manual).
- A password policy must be implemented. Passwords may not be stored in plain text. Passwords may be stored only in hashed form. The hash algorithm shall apply the latest technology.
- For every application, a concept for recording logs shall be documented (e.g. in the operating manual), ensuring that the logs are recorded in a standard format. As a minimum, the following events shall be recorded:

- successful and failed logins
- changes to permissions and roles
- user administration activities
- other security-related events in the application.

Service provider Dependency and subcontractor engagement

- All requirements shall also apply to any subcontractors and consortium partners involved.
- In case of engaging a subcontractor, the service provider must assess the suppliers by evaluating their compliance with requirements as stated in this contract. The contractor remains fully liable for subcontractor actions.
- A subcontractor cannot be engaged without approval of the GIZ and the MINALOC.
- If approved, subcontractor must sign a Non-Disclosure Agreement (NDA) with the MINALOC.