

Terms of Reference and Request for Proposal

For the Design, Development, Deployment and Support of a Secure Digital Victims' Registry for Survivors of Conflict-Related Sexual Violence in Sudan

Contracting organisation	The Global Fund for Survivors of Conflict-Related Sexual Violence (Global Survivors Fund / GSF)
Tender reference no.	REG/TEND/2026/10
Implementation context	Sudan, with implementation on location through AWAFFY Sudanese Organization and trusted Sudanese civil society partners.
Target areas	Darfur, Kordofan, Khartoum, Northern State and Blue Nile.
Project timeline	18-month project, beginning on 01 November 2026; The Live environment must be deployed within five months of project commencement (March-April 2027); Supplier implementation must fit the project schedule and support long-term continuity.
Procurement method	Open competitive tender.
Financial information	No ceiling or indicative budget is disclosed. Bidders must provide a competitive, fully itemised financial proposal.
Submission information	Please send your submissions as a PDF package to opentender@globalsurvivorsfund.org by 27 October 2026, by 11:59 PM (CET), with the reference number REG/TEND/2026/10 in the email subject.
Contact focal point	Vishnu Varatharajan, Programme System Officer

This Request for Proposal (RFP) seeks a qualified software supplier to provide a secure, survivor-centred, offline-capable and interoperable registry solution. Architectural and security design may begin immediately after contract signature. However, the registry's substantive design, including data fields, workflows, eligibility logic, consent, verification and access arrangements, must be co-created with survivors of conflict-related sexual violence and cannot be treated as fixed before that process.

Contents

1. Background and purpose	3
2. Procurement objective.....	3
3. Guiding principles and non-negotiables	4
4. Scope of work	4
4.1 Orientation, requirements scoping and architecture	4
4.2 Survivor co-creation and design translation	5
4.3 Registry application and workflows.....	5
4.4 Identification, verification and de-duplication.....	6
4.5 Security, privacy and data protection	6
4.6 Availability and operational resilience.....	7
4.7 Interoperability and future handover	7
4.8 Training, documentation, support and knowledge transfer.....	7
5. Indicative user, workload and geographic assumptions	7
6. Deliverables and acceptance criteria.....	8
7. Indicative implementation sequencing	9
8. Governance and working arrangements	9
9. Data ownership, confidentiality and intellectual property	10
10. Safeguarding and ethical requirements	10
11. Supplier qualification requirements.....	10
12. Proposal submission requirements	11
12.1 Technical proposal.....	11
12.2 Supplier and team information.....	11
12.3 Financial proposal	12
13. Evaluation methodology	12
14. Mandatory tender conditions	12
Annex A. Requirements compliance matrix	13

1. Background and purpose

Sudan currently lacks a systematic, consented, reparations-oriented digital record for survivors of conflict-related sexual violence (CRSV). GSF and AWAFFY Sudanese Organization (AWAFY) are implementing an 18-month project to establish a secure Victims' Registry that supports recognition, confidential documentation, access to urgent reparative measures and a durable evidentiary foundation for future reparation and accountability processes. The registry is intended to outlast the initial project and be capable of scaling substantially beyond the proof-of-concept phase.

The operating environment is exceptionally sensitive. Survivors may face stigma, repeated displacement, distrust of formal institutions, disrupted services, information blackouts and low or intermittent internet connectivity. Consequently, survivor safety must take precedence over scale, data minimisation must be applied from data collection onward, and the data collection solution must work through de-centralised field operations rather than requiring continuous connectivity or centralised physical collection.

During the project, approximately 500 survivors of conflict-related sexual violence are expected to be documented in the registry and supported through case management. The system must nevertheless be architected for hundreds of thousands of additional records and future expansion to other survivor populations without re-platforming. At least 20 staff from 10 authorised Sudanese CSOs are expected to be enabled to contribute to the registry, with a wider cohort of 40 partner-organisation staff, community actors and facilitators expected to receive training on secure and ethical data collection, case management and referral management. Five registration staff and five caseworkers are planned in the field team, alongside psychologists and safe-space facilitators. These user numbers are procurement sizing assumptions, not limits on licensing or scalability.

2. Procurement objective

GSF invites proposals from experienced software suppliers to design, develop, test, deploy, and support the digital Victims' Registry. The supplier will coordinate with GSF's Senior Technical Registry Officer, with operational input from AWAFFY and validation from survivor representatives and other relevant GSF staff.

- Translate the co-created requirements arising out of the survivors workshop into technical specifications for the digital registry. without prematurely constraining co-creation outcomes.
- Provide a robust architecture and secure cloud hosting located outside Sudan.
- Propose the hardware and software required based on this RFP along with costing.
- Enable confidential, decentralised and offline data collection with controlled synchronisation.
- Provide strong identification, verification and de-duplication mechanisms appropriate for a high-risk survivor registry.
- Enable role-based workflows for intake, verification, case management, referrals and reporting.
- Deploy the Live environment within 5-months of project commencement (March-April 2027).
- Ensure interoperability so that data and operations can be handed over in future to an appropriate custodian, such as a credible national reparations body or an international organisation, subject to GSF's governance decisions and survivor consent.
- Build maintainable institutional capacity, avoiding over-dependence on a proprietary supplier.

3. Guiding principles and non-negotiables

The following table briefs the guiding principles of the project. Some of them may not be directly relevant to the development of the registry, but may provide additional context to the supplier:

Principle	Required application
Survivor-centred co-creation	Survivors have a decisive role in determining what is collected, how it is collected and used, access arrangements, eligibility and verification. Supplier must accommodate iterative decisions.
Do no harm	Safety, dignity and confidentiality is paramount. The solution must reduce risks arising from device compromise.
Informed consent and agency	Consent must be intelligible, granular, auditable and revocable where applicable. Participation is voluntary and does not itself guarantee assistance or future reparations.
Data minimisation and privacy by design	Collect only justified data; separate identifying data from sensitive case narratives where appropriate; apply privacy controls from the beginning.
Presumption of good faith	Verification is not a judicial proof exercise and must not create unnecessary burden or require survivors to repeatedly recount violence, minimising or completely avoiding retraumatisation.
High security by design	Encryption, MFA, auditability, secure cloud architecture, and incident procedures are baseline requirements.
Local usability	The system must perform in low-connectivity environments, support Arabic and English at minimum, and be usable by trained location staff under constrained conditions.
Portability and sustainability	GSF must be able to export data, configurations and documentation in open/standard formats and transfer to a successor custodian without the risk of supplier lock-in.

4. Scope of work

4.1 Orientation, requirements scoping and architecture

- Conduct orientation with GSF and AWAFFY, and confirm governance, IT and location stakeholders, project assumptions, dependencies, implementation plan and the risk register.
- Undertake requirements scoping, covering operations, security threats, data protection, safeguarding, user roles, workflows, reporting, integration and future custodianship.

- Produce system and security architecture, data-flow diagrams, data classification scheme, access model, backup and disaster-recovery design.
- Prepare an architecture that permits early work on environment, security, hosting, and deployment pipelines and generic platform capabilities while preserving flexibility for survivor co-design decisions.
- Identify proposed third-party services, hosting regions, software dependencies and licensing implications. Open-source or widely interoperable technologies are preferred where suitable.

4.2 Survivor co-creation and design translation

A key design workshop will be held with survivors and relevant Sudanese civil society actors in a safe, accessible location such as Kampala, supplemented by consultations through existing community networks. The supplier must participate technically and translate validated inputs into the product design. The detailed registry design is therefore a deliverable following co-creation.

- Provide accessible prototypes and workflow options suitable for non-technical validation.
- Capture and maintain a requirements decision log and traceability matrix showing how survivor inputs affect design.
- Support decisions on data categories, survivor control, verification, case-management workflow and permissions.
- Adapt GSF's survivor identification forms into the digital solution after validation.
- Prototype sensitive workflows and run usability testing with authorised GSF staff.

4.3 Registry application and workflows

- Multilingual intake using a single underlying data structure with language-specific labels; Arabic and English minimum, with extensibility for additional languages.
- Primarily structured fields for consistent data quality and analysis, with controlled free-text where qualitative information is necessary.
- Configurable forms, conditional logic, validation, versioning and change control where necessary.
- Offline data capture with encrypted local storage for the minimum necessary period, reliable synchronisation when connectivity returns, and sync status.
- Unique, non-overlapping survivor identifiers (IDs) that also minimise exposure of identity.
- End-to-end workflow states such as draft, submitted, review required, verified/eligible, not eligible, registered, closed, etc. subject to final co-design.
- Capability to record each interaction as a distinct event to maintain longitudinal history of registration, case management, referrals and urgent reparative measures without overwriting prior events.
- Tasking, case assignment, follow-up dates, referral tracking and status.
- Configurable referral directory and referral tracking, while avoiding disclosure of sensitive data to external services without authorised consent.
- Aggregate dashboards and reports that do not expose identifiable information unless explicitly permitted.
- Export capability for anonymised/aggregated analysis if needed.

4.4 Identification, verification and de-duplication

The registry requires a particularly strong identification and verification mechanism. Bidders must propose an approach that increases confidence that a survivor can be safely re-identified over time and reduces duplicate records while avoiding unnecessary collection of high-risk identifiers.

- Configurable identity matching and de-duplication, duplicate alerts with a merge/link workflow and the ability to correct an erroneous match.
- Support separation of identity information from case narratives and use pseudonymous identifiers/tokens across operational views where needed.
- No supplier use of registry data, survivor identity, metadata for AI/model training, product analytics, advertising or unrelated purposes.

4.5 Security, privacy and data protection

- Secure cloud hosting outside Sudan, with data-residency options declared in the proposal and approved by GSF before production. Bidder must describe availability architecture, redundancy, backups, monitoring, capacity and failure modes.
- Encryption in transit using current secure protocols and strong encryption at rest, including databases, backups, and any offline caches holding sensitive data.
- Central identity management for authorised staff; Role-based Access Control (RBAC) and mandatory Multi-Factor Authentication (MFA) for registry access; possible access revocation by administrators; configurable session timeout.
- Multiple role profiles such as data collector, case manager, registry officer, data protection officer, reporting/MEL, viewer, system administrator, etc, with final roles determined during design.
- Technical supplier staff must have no standing unilateral access to survivor data. Any exceptional support access must be time-bound, approved, limited, logged and reviewable.
- Immutable or tamper-evident audit trail for authentication, creation, modification, export, deletion, permission changes and administrative actions, with timestamp and user identity.
- Backups encrypted and tested; documented recovery objectives proposed by bidder and confirmed at design stage; restoration exercises in test environment before go-live, with no real survivor data during development or routine test environments.
- Independent penetration testing before go-live and after any security changes, with remediation evidence. GSF must receive the relevant executive and technical findings.
- Incident detection, logging, alerting, having incident response guidelines and rapid notification to GSF.
- High-level configurable retention, suspension, deletion and migration procedures to respond to security deterioration or future custodianship decisions.
- Support for data management and privacy obligations consistent with the project's GDPR-alignment and [Murad Code](#) principles.

4.6 Availability and operational resilience

- Design for intermittent connectivity. Sensitive records must not remain indefinitely on collection devices; sync and secure purge policies must be defined.
- Support controlled remote disablement where feasible and clear device security requirements for location operations.
- Provide monitoring for application health, sync failures, storage, database performance and suspicious authentication.
- Capacity plan must demonstrate comfortable handling of the initial 500 survivor records, expected operational users, and growth to hundreds of thousands of survivor records without fundamental redesign.

4.7 Interoperability and future handover

- Documented APIs or secure exchange mechanisms using common open standards/formats.
- Data dictionary, schema, code lists, configuration exports and migration specifications delivered to GSF.
- If needed, the ability to create custom exports and anonymised/aggregated datasets for reporting processes.
- Exit plan enabling migration to another platform, an international organisation or a future national reparations authority without loss of provenance, audit history or data integrity.

4.8 Training, documentation, support and knowledge transfer

- Role-based training for administrators, data collectors and case managers. Training-of-trainers capability is strongly preferred.
- User guidance in English and Arabic for relevant operational roles, including offline/sync procedures and safe handling.
- Administrator, API, security, backup/restore, incident-response and troubleshooting documentation.
- Maintenance and support through the agreed project period, including ticketing, security patching and periodic health reviews.
- Handover sessions sufficient for GSF or a future custodian to administer the system and perform exports/migration without supplier dependency.

5. Indicative user, workload and geographic assumptions

Item	Planning basis for proposal
Survivors registered during project	Approximately 500, with architecture designed for hundreds of thousands more
Authorised CSOs contributing to registry	10 organisations
Direct CSO contributors	At least 20 people, minimum two per authorised CSO

Item	Planning basis for proposal
Wider people trained in data collection/case management/referral	40 partner staff and peer facilitators
Dedicated registration staff	5
Dedicated caseworkers	5
Other roles	5 psychologists and 5 safe-space facilitators; access needs to be confirmed according to role
Regions	Darfur, Kordofan, Khartoum, Northern State and Blue Nile
Connectivity	Low/intermittent connectivity and information blackouts must be assumed
Scaling-up	System must support future expansion and successor custodianship without re-platforming

6. Deliverables and acceptance criteria

No.	Deliverable	Minimum acceptance criteria
D1	Inception package	Workplan, governance, risk/dependency registers, stakeholder plan and delivery method approved by GSF.
D2	Architecture and security baseline	Target architecture, threat model, data flows, environments, hosting/data residency, RBAC, encryption/key management, backup/DR, logging/monitoring, hardware devices/offline security approved by GSF.
D3	Co-creation design pack	Validated requirements, workflow diagrams, prototype, user roles, consent/eligibility/verification implementation, decision log and traceability to survivor inputs.
D4	Configured/developed alpha/beta	Core intake, offline/sync, identification/deduplication, verification, case/event history, referrals, RBAC, audit, multilingual UI and reporting are demonstrable in non-production environment.
D5	Security and performance assurance	Vulnerability scans, independent penetration test, backup/restore test, load/capacity testing and documented residual risks approved by GSF.

No.	Deliverable	Minimum acceptance criteria
D6	Production go-live	Secure cloud environment, approved configuration, monitoring, backup, runbooks, and controlled migration of approved configuration to live.
D7	Training and documentation	Role-based training completed; editable training materials, Arabic/English user guidance as applicable, and technical/admin documentation.
D8	Operational support and iterative refinement	Agreed support SLAs met; security patches maintained; issues and enhancement backlog managed; refinement incorporates GSF approved feedback from location.
D9	Handover and exit package	Current source/configuration as contractually applicable, data exports, dictionary/schema, credentials/key transfer procedure, security workflows, operations documentation, migration/handover procedure and knowledge-transfer sessions.

7. Indicative implementation sequencing

Bidders should propose a realistic schedule aligned with the 18-month project. The following sequencing expresses dependencies rather than fixed contract dates.

- Immediately from contract signature: inception; risk/threat assessment; cloud, network; environment setup; generic offline/security prototyping.
- Before and around the survivor co-creation workshop: prepare prototypes and design choices without locking substantive registry rules. Participate in workshop and consultations.
- Immediately after survivor validation: finalise requirements, data model, workflows, role matrix and forms; develop/configure the registry iteratively.
- Test phase: controlled UAT, user training, security testing, feedback and remediation. Registration should only begin once GSF formally authorises production use.
- Operational phase: Scaled registration, continuous support, security monitoring, refinements and capacity strengthening.
- End phase: Sustainability, migration readiness, full handover and exit documentation.

8. Governance and working arrangements

- GSF will lead technical design ownership, registry system management, data protection governance and overall programme oversight.
- AWAFFY will provide operational requirements on location, and coordinate system's usage on location with authorised Sudanese CSOs.
- GSF's Senior Technical Registry Officer is expected to be the principal technical counterpart and supplier manager.

- A steering committee involving relevant actors will provide strategic and ethical oversight.
- A Technical Secretariat is expected to review/verify applications against defined criteria on a regular basis.
- The supplier shall attend agreed design, sprint/review, security and steering meetings and maintain concise decision, risk and action logs.
- All changes affecting sensitive data, permissions, verification policy, interoperability or hosting require explicit written approval from GSF.

9. Data ownership, confidentiality and intellectual property

- All survivor data, case data, metadata, configurations specifically created for GSF, and project-generated documentation are controlled by GSF under applicable agreements. The supplier acquires no independent rights to use them.
- The supplier and its personnel/sub-processors must sign appropriate confidentiality and data-processing commitments.
- The supplier must disclose all sub-processors and locations where project data may be stored, backed up, logged, accessed or supported, and changes require written approval from GSF.
- Bidders must state proposed intellectual-property/licensing terms. GSF requires perpetual access to project data and documentation and sufficient rights to maintain, migrate and handover the solution.
- No lock-in: Termination/expiry of software must not inhibit export of complete, intelligible data and configurations or require payment of unreasonable extraction fees.
- All non-production demonstrations during tendering must use synthetic data only.

10. Safeguarding and ethical requirements

- Design must support survivor-centred, trauma-informed operations, safeguarding, PSEA and child-safeguarding requirements.
- Minimise repeated requests for survivors to recount traumatic experiences. Users should retrieve prior authorised information rather than re-interview unnecessarily.
- Where children/adolescents are within approved eligibility, the solution must support age-appropriate consent/assent and additional confidentiality controls as defined by project protocols.
- System notifications, screen labels, device caches and exported file names should avoid revealing unnecessarily that a person is a survivor of conflict-related sexual violence.

11. Supplier qualification requirements

The bidder, or a clearly defined consortium, should demonstrate the following. Evidence should distinguish the proposed team's direct experience from general corporate claims.

- Demonstrated delivery of secure case-management, registry, protection, health, humanitarian, justice, human-rights or similarly sensitive systems.
- Demonstrated cloud security, privacy engineering, RBAC, encryption, audit logging, backup/DR and secure software development capability.
- Demonstrated offline-first/mobile data collection and synchronisation in low-connectivity environments.

- Experience implementing privacy-preserving identity matching, de-duplication or verification workflows.
- Strong data protection and GDPR capability; experience with highly sensitive data is strongly preferred.
- Ability to work ethically with survivor-centred projects and translate participatory/co-created requirements into iterative product design.
- Capacity to provide secure support across relevant time zones and throughout implementation.
- Ability to deliver robust technical and user documentation and transfer knowledge.

12. Proposal submission requirements

Proposals should be sufficiently detailed to permit comparative technical, security, delivery and financial evaluation.

Please send your submissions as a PDF package to opentender@globalsurvivorsfund.org

Submissions must be received by 27 October 2026, by 11:59 PM (CET), with the reference number REG/TEND/2026/10 in the email subject.

You may contact us at the email address above with any questions you may have during the preparation of your application. Please note that the questions received and our responses will be shared with all applicants who have expressed an interest in submitting a bid, so that all known applicants have equal access to relevant information

12.1 Technical proposal

- Executive summary and understanding of the assignment and risk context.
- Proposed solution and architecture, including whether configuring an existing product, extending an open-source platform, developing custom components, or a hybrid.
- Detailed response to every mandatory requirement in Annex A using Comply / Partially comply / Do not comply / Requires configuration or development, with explanatory evidence.
- Proposed client co-creation and iterative design methodology.
- Identification, verification and de-duplication mechanisms.
- Security and privacy approach, cloud provider/region options, encryption/key management, access model, audit, incident response, SDLC, penetration testing, backup/DR and data lifecycle.
- Offline/synchronisation approach and field device assumptions.
- Interoperability/API, data portability and exit strategy.
- Implementation plan with milestones, dependencies, resource plan and proposed delivery schedule.
- Training, documentation, maintenance/support and SLA proposal.

12.2 Supplier and team information

- Company/consortium profile, legal registration, ownership and principal operating locations.
- At least two relevant reference projects, preferably involving sensitive data, registries/case management, humanitarian/conflict settings or low-connectivity deployments.

- Named project manager, solution architect, security/privacy lead, lead developer/configurator, QA/test lead and training/support lead, with CVs and confirmed availability.
- Description of quality, information-security and privacy management practices and relevant certifications, if any.
- Disclosure of actual or potential conflicts of interest.

12.3 Financial proposal

The bidder must submit a complete and competitive financial proposal that makes the full cost of ownership transparent.

- One-time discovery, design, configuration/development, testing, security assurance, training and go-live costs.
- Cloud hosting/infrastructure, licenses/subscriptions and third-party service costs, itemised by unit and period where possible.
- Maintenance/support costs and any optional support tiers.
- Taxes/VAT status and currency.
- Rate card for additional work.
- Optional proposed features priced separately.
- Any cost that could arise on data export, migration, handover or termination.

13. Evaluation methodology

Award will be made to the most economically advantageous compliant proposal, considering quality and total cost rather than lowest price alone. GSF may conduct clarification interviews, technical demonstrations, reference checks and security due diligence before award.

Criterion	Indicative weight
Technical fit, including implementation method, team and relevant experience	25%
Security, privacy, cloud architecture and resilience	20%
Identification, verification and de-duplication approach	15%
Interoperability, sustainability, support and handover	20%
Financial proposal and total cost of ownership	20%

GSF reserves the right to treat critical security, confidentiality, data residency, survivor-safety, data ownership/portability, offline capability, or material non-compliance as grounds for rejection regardless of aggregate score.

14. Mandatory tender conditions

- Bidders shall not contact survivors, Sudanese field partners or other project stakeholders independently for proposal preparation. Any access required will be organised by GSF.

- Bidders must complete the Requirements compliance matrix given below in Annex A and indicate for each requirement whether it is fully met, partially met, requires configuration or development, or cannot be met.
- GSF may amend or cancel the procurement, request clarifications, negotiate minor contractual, technical and implementation details with the preferred bidder prior to contract signature, and conduct due diligence in accordance with its procurement rules.
- The successful bidder will be required to comply with applicable safeguarding, confidentiality, data protection, information security, restrictive-measures and conflict-of-interest requirements.

Annex A. Requirements compliance matrix

Priority: M = mandatory; C = conditional/optional subject to GSF approval and survivor consultation.

Functional: F-01 to F-09, Security: S-01 to S-09, Interoperability: I-01 to I-03, Operational: O-01 to O-05,

Design/co-creation: D-01

ID	Priority	Requirement	Bidder response/evidence
F-01	M	Offline-capable data entry and secure synchronisation when connectivity becomes available.	
F-02	M	Arabic and English user interface/labels using a consistent underlying data structure; extensible multilingual design.	
F-03	C	Configurable structured intake, validation/conditional logic and controlled qualitative free text.	
F-04	C	Longitudinal event history for survivor interactions, registration, referral and follow-up.	
F-05	C	Configurable survivor consent capture and consent history.	
F-06	M	Case assignment, review and verification, formal registration and follow-up workflow.	
F-07	M	Strong identity matching and de-duplication, with potential duplicate records flagged for authorised human review. Where records are linked or merged, the system must preserve the original records, source information and audit history, and record who authorised the action and when.	
F-08	M	Pseudonymous/unique identifiers and separation of identifying data from case narratives where needed.	
F-09	M	Aggregated/anonymised reporting and controlled exports. Or	

ID	Priority	Requirement	Bidder response/evidence
		better, a secure, limited external access mechanism to selected fields so that the data remain in a single warehouse, and not exported out.	
S-01	M	Secure cloud hosting outside Sudan; full disclosure of hosting and backup locations.	
S-02	M	Encryption in transit and at rest, including backups and offline caches.	
S-03	M	MFA, RBAC. Sensitive responsibilities should be appropriately separated between different user roles. The system must also allow authorised administrators to promptly suspend or remove a user's access when they leave the project, change roles, or no longer require access.	
S-04	M	Comprehensive tamper-evident audit trail and administrative logging.	
S-05	M	No supplier access to identifiable survivor data.	
S-06	M	Independent penetration test before go-live, and ongoing vulnerability management.	
S-07	M	Encrypted backup, tested restore, incident response, monitoring and security alerting.	
S-08	M	Configurable retention, deletion, data suspension and migration controls.	
S-09	M	No use of project data for supplier analytics, AI/model training, advertising or unrelated purposes.	
I-01	M	Open/standard export of complete data, dictionary/schema, audit and configuration sufficient for migration.	
I-02	M	Documented APIs or secure interoperable exchange mechanisms.	
I-03	M	Future custodianship/handover without proprietary lock-in.	
O-01	M	Scales from 500 initial survivors to hundreds of thousands without fundamental redesign.	
O-02	C	Training and support for authorised CSOs and users on location.	

ID	Priority	Requirement	Bidder response/evidence
O-03	C	Arabic/English operational guidance as required and full technical/admin documentation.	
O-04	M	Support SLA, ticketing, patch management and service-health monitoring.	
O-05	M	Deploy the Live environment within 5-months of project commencement (March-April 2027).	
D-01	M	Supplier supports gated co-design: architecture may start early, but final data/workflow/eligibility/verification design follows survivor co-creation and approval.	

The opening of bids will take place on Wednesday, 28 October 2026. Qualified vendors will be contacted to schedule a presentation/demo.

We are looking forward to receiving your proposals and potentially collaborating on this crucial project to develop a Digital Victims' Registry for Survivors of Conflict-Related Sexual Violence in Sudan.

Sincerely,

The Global Survivors Fund