AVOCATS SANS FRONTIÈRES FRANCE

EXPRESS Project
Enhancing eXpression and Protection of Rights in the Evolving Digital Space Project

Call for Tenders: Establishment of a 'Cybercrimes Act Barometer' to monitor the use of the Cybercrime Act during and after the election campaign

TERMS OF REFERENCE

November 2026

Full legal name (company name)	AVOCATS SANS FRONTIERES France (*Lawyers without borders France*)
Acronym	ASF France
Legal status	Association governed by the 1901 Act
Address	13 Rue des Fleurs 31000 Toulouse France
Contact person	Angela UWANDU UZOMA-IWUCHUKWU Head of Office
Phone number	+234 (0) 703 782 8203
Email address	office.nigeria@avocatssansfrontieres-france.org
Project title	Enhancing eXpression and Protection of Rights in the Evolving Digital Space Project (EXPRESS Project)
Main donor	Embassy of the Netherlands in Nigeria
Project start and end dates	30 November 2026 – 25 April 2027
Deadline for submission of tenders	24 November 2026
Application email	recrutements@avocatssansfrontieres-france.org

Table of contents

1. Introduction 4

Avocats Sans Frontières France 4

EXPRESS Project 4

Context 4

2. Purpose and Objectives of the Assignment 5

Rationale for the assignment. 5

Objectives 5

Methodology 5

3. Timetable 6

4. Deliverables 7

5. Expert profile 8

6. Budget, payment and contract terms 8

7. Evaluation of the tender 9

8. Intellectual property and confidentiality 9

9. Tender submission procedure 9

10. How to submit 9

1. Introduction

Avocats Sans Frontières France

Avocats Sans Frontières France (Lawyers Without Borders France / ASF France) is an international non-governmental organisation dedicated to defending fundamental human rights, supporting vulnerable populations, and reinforcing the rule of law. Operating in Nigeria since 2005, ASF France focuses on improving access to justice and combating human rights violations across the criminal justice system. Grounded in a holistic approach to justice sector reform, ASF France addresses interrelated issues such as torture, arbitrary detention, capital punishment, and gendered injustices, while expanding its core mandate to safeguard digital rights and press freedom. Building on its extensive experience defending civic space, ASF France's recent work, including through the EXPRESS and e-RIGHTS projects, aims to foster a safer and more rights-respecting digital environment in Nigeria. By strategically leveraging technology as a tool for advancing law, human rights defence, and accountability, the organisation combats the disproportionate restriction of digital rights, protects journalists and activists from arbitrary enforcement, and ensures that cybersecurity regulations uphold fundamental freedoms, privacy, and due process.

EXPRESS Project

The "Enhancing eXpression and Protection of Rights in the Evolving Digital Space Project" – EXPRESS project (2026-2029), supported by the Embassy of the Netherlands in Nigeria, aims to contribute to a safer and more rights-respecting digital environment in Nigeria by promoting the effective, fair, and technically informed implementation of the Cybercrimes Act. It seeks to strengthen the ability of legal and justice sector actors to respond effectively to cybercrime and protect genuine victims, while ensuring that the enforcement of cybercrime legislation respects fundamental rights and freedoms, including freedom of expression, privacy, and due process. Through legal research, capacity strengthening, strategic advocacy, and multi-stakeholder engagement, the project promotes a balanced and evidence-based approach to cybercrime regulation that addresses genuine cyber threats while preventing the disproportionate or unlawful restriction of digital rights.

Context

Nigeria's Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 (as amended in 2024) was enacted to combat cybercrime by criminalising offenses committed through computer systems, protecting critical national information infrastructure, and safeguarding Nigerians in cyberspace. However, concerns have been raised by civil society organisations, human rights defenders and international stakeholders regarding the use of certain provisions of the Act, particularly Section 24 on cyberstalking, to investigate or prosecute journalists, activists and individuals expressing critical opinions online, both before and after the 2024 amendment. Meanwhile, genuine victims of cybercrime, particularly women, elderly citizens, and rural users, rarely obtain justice. Today, there is no single, reliable source of data on how the Act is enforced, who is charged, under which provisions, and with what outcomes. The Barometer will close that gap.

2. Purpose and Objectives of the Assignment

Rationale for the assignment.

The Barometer will be a publicly accessible, searchable, and continuously updated database of prosecutions, investigations, and judicial decisions arising under the Act, generating reliable longitudinal evidence on enforcement patterns. It will function as both a transparency tool and an analytical resource, enabling lawyers, journalists, researchers, policymakers, and affected citizens to understand how the law is being applied in practice. Each case entry will capture, where available: defendant profile, specific provision invoked, originating complaint (state-initiated or private), location and court, arrest and detention details, bail conditions, duration of pre-trial detention, charges, verdict, sentence, and appeals. Cases will be thematically tagged to enable disaggregated analysis. The Barometer will be implemented exclusively in the three project target states: Abuja, Lagos and Enugu states to ensure focused monitoring and effective data collection. Restricting the platform's initial scope allows for direct engagement with local judicial stakeholders, establishing a rigorously tested model that can be scaled up across other states under future initiatives. This focused approach also ensures that technical resources and legal support are concentrated where they can generate immediate, measurable impact rather than being stretched thin across the nation.

The Barometer will provide open-data export and API access and will serve as an authoritative reference on the state of the Cybercrime Act in Nigeria. A dynamic cross-analysis will help to facilitate understanding of the cases and provide the data needed to assess the application of the CyberCrimes Act in relation to human rights.

It serves two functions:

- **Transparency tool:** lets lawyers, journalists, researchers, policymakers and affected citizens see how the law is applied in practice.
- **Analytical resource:** supports dynamic cross-analysis of cases to assess the Act's application against human rights standards.

Objectives

The expert will deliver a fully functioning, publicly accessible tool (Barometer), populated with verified case data from the three target locations, and hand it over to ASF France for sustained operation.

Specific objectives:

1. Design a robust methodology and data model for documenting Cybercrimes Act cases, grounded in human rights standards.
2. Build a secure, searchable, mobile-friendly web platform with open-data export and a public API.
3. Establish data collection and verification protocols with courts, lawyers, and civil society in Abuja (FCT), Lagos and Enugu.
4. Populate the Barometer with an initial verified dataset of cases.
5. Develop analytical dashboards and cross-analysis features that show enforcement patterns and human rights impact.
6. Train ASF France staff and partners to update, maintain and analyse the Barometer independently.
7. Monitor the platform for three months after the project to resolve any technical issues that may arise.

The Barometer must be capable of being transferred to a larger platform dedicated to digital rights, which will be set up by ASF France in early 2027.

Methodology

The work runs in five phases. The expert will work closely with the EXPRESS project team and report to the Project Manager.

Phase 1: Inception and methodology

- Review the Cybercrimes Act (as amended), relevant case law, and existing monitoring initiatives in Nigeria and comparable jurisdictions.
- Map data sources in each target location: court registries, Ministry of Justice and police records, defence lawyers, media reports, CSO case files, and affected persons.
- Define the data model, field definitions, controlled vocabularies and the thematic tagging taxonomy (e.g. journalism, political criticism, cyberstalking (Section 24), gender, protest).
- Set verification standards, source-rating rules, and a protocol for handling incomplete or contested information.
- Develop a data protection and do-no-harm framework compliant with the Nigeria Data Protection Act 2023, including rules on anonymisation, consent, and protecting defendants and sources.

Phase 2: Platform design and development

- Design the information architecture and user interface with input from target users (lawyers, journalists, researchers).
- Build the database and public web platform with full-text search, filters (provision, location, court, year, outcome, defendant category, tag) and case detail pages.
- Build open-data export (CSV, JSON) and a documented public API.
- Build interactive dashboards and cross-analysis tools, e.g. charges by provision over time, pre-trial detention duration by location, conviction rates by complaint origin.
- Provide a secure back-end for data entry, review and approval, with role-based access and an audit trail.
- Use open-source technologies where possible, ensure accessibility (WCAG 2.1 AA), and apply security best practices (encryption, backups, penetration testing).

Phase 3: Data collection and population

- Engage judicial stakeholders, bar associations and CSOs in Abuja, Lagos and Enugu to secure access to case information.
- Develop data collection tools.
- Collect, verify and enter an initial dataset of cases [target number to be agreed at inception], including historical cases where available.

Phase 4: Testing and launch

- Run user acceptance testing with a pilot group of stakeholders and fix issues found.
- Support the public launch, including a baseline analytical brief on enforcement trends in the three locations.

Phase 5: Handover and capacity building

- Deliver technical documentation, user manuals and a methodology handbook.
- Train ASF France staff and partners on data entry, verification, platform administration and analysis.
- Transfer all source code, credentials, hosting accounts and data to ASF France.
- Provide post-launch technical support and maintenance for 3 months [to be confirmed].

3. Timetable

Below is an indicative timetable for the project:

Phase	Timeline
Launch of the call for tenders	10 November 2026
Deadline for applications	24 November 2026
Start of the assignment	30 November 2026
Phase 1: Inception and methodology	30 November - 5 December 2026
Phase 2: Platform design and development	7 December 2026 – 3 January 2027
Phase 3: Data collection and population	4 – 22 January 2027
Phase 4: Testing and launch	4 – 22 January 2027
Phase 5: Handover and capacity building	25 January – 25 April 2027

Consultants must specify the stages and the number of working days allocated to each stage in their technical proposal by means of a timetable.

4. Deliverables

1- Inception and Methodology Report

A comprehensive inception report setting out the monitoring methodology, case selection criteria, data model, classification and tagging system, verification procedures, and data protection framework. The report shall also include a detailed work plan, stakeholder mapping, data collection strategy and risk mitigation measures, subject to ASF France's approval.

2- Platform Design and Functional Prototype

A validated technical architecture and platform prototype, including wireframes, database structure, user interface and core functionalities, demonstrating the proposed approach to data management, case search and visualisation. The prototype shall be reviewed and approved by ASF France before proceeding with full development.

3- Fully Functional Cybercrimes Act Barometer

A fully operational, secure and publicly accessible web platform, including searchable case records, filtering tools, analytical dashboards, open-data export functionalities and a documented API. The platform shall be designed to ensure interoperability and facilitate its future integration into ASF France's broader digital rights platform.

4- Verified Dataset, Testing and Analytical Report

An initial dataset of documented and verified cases from Abuja (FCT), Lagos and Enugu shall be collected, analysed and uploaded to the Barometer, in accordance with the methodology approved by ASF France. This deliverable shall also include user acceptance testing, a report on the platform's performance and a baseline analytical report highlighting key trends and human rights implications in the application of the Cybercrimes Act.

5- Handover, Capacity Building and Technical Support

A complete handover package comprising the source code, technical documentation, user manuals, database, credentials and administrative access, ensuring ASF France's full ownership and independent management of the platform. The consultant shall train ASF France staff and designated partners in platform administration, data collection, verification and analysis, and provide three months of post-launch technical support and maintenance. The consultant must facilitate the migration of the Barometer to a broader platform in 2027.

All reports are to be submitted in English, in editable format. All data, code and materials produced become the property of ASF France and should be released under an open licence agreed with the organisation.

5. Expert profile

The assignment combines legal, research and technical skills. Individual experts may apply, but a small team (or a lead expert with named or un-named sub-consultants) is encouraged.

Essential

- Advanced degree in law, human rights, data science, computer science, or a related field.
- At least 7 years' relevant experience, including at least one comparable legal or human rights monitoring database, tracker or observatory.
- Demonstrated knowledge of the Nigerian Cybercrimes Act, criminal procedure (including the Administration of Criminal Justice Act 2015), and freedom of expression standards.
- Proven experience building secure, searchable web databases with public APIs and data visualisation.
- Proven experience in building front-end web applications.
- Experience in legal research and court monitoring in Nigeria, ideally in the FCT, Lagos or Enugu.
- Sound knowledge of data protection, research ethics and digital security when handling sensitive data.
- Excellent written English and analytical skills.

Desirable

- Existing networks with courts, the Nigerian Bar Association, media and digital rights organisations.
- Experience with open-data standards and open-source platforms.
- Prior work with NGOs or donor-funded projects.

6. Budget, payment and contract terms

The budget must be proposed by the consultant(s) and set out in detail in their tender.

Payment shall be in instalments tied to progress of work. The final payment shall be made after the full platform has been accepted and the maintenance carried out.

7. Evaluation of the tender

The tender will be evaluated on a total of 100 points. This comprises the evaluation of the technical proposal (75 points) and the financial proposal (25 points). The proposals submitted will be evaluated by the selection committee using a cumulative analysis method.

a) Technical proposal (75 points)

1) The consultant(s)' experience relevant to the assignment – *20 points*
2) Alignment of the proposed methodology and work plan with the terms of reference – *40 points*
3) Qualifications and skills of the consultant(s) for the assignment – *15 points*

b) Financial proposal (25 points)

1) Amount of the financial proposal (Np = 10 x Pm/ P, where "Np" is the price score, "Pm" is the lowest price, and "P" is the price of the proposal being assessed) – *10 points*
2) Consistency of the budget with the proposed methodology – *8 points*
3) Reasonableness and proportionality of costs – *7 points*

The three best proposals will be shortlisted for a selection interview in late November 2026.

8. Intellectual property and confidentiality

- **Intellectual property:** All outputs become the property of ASF France. The expert(s) will be credited as author.
- **Confidentiality:** Information obtained during the assignment may not be disclosed without written consent.

9. Tender submission procedure

The application dossier shall consist of:

- A **technical proposal**, setting out the scope of the study (understanding of the terms of reference, the methodology to be used, the risks identified and the proposed mitigation plan, the timetable and the proposed work plan) – 10 pages maximum.
- A **financial proposal** separate from the technical proposal, inclusive of all taxes and covering field travel, food, accommodation, etc. – max. 2 pages.
- The **CVs** of the consultant(s) – max. 4 pages per consultant
- If possible, **two references** from similar consultancy projects previously carried out (submitting extracts from past work is an advantage).

10. How to submit

Tenders should be sent to recrutements@avocatssansfrontieres-france.org with the subject line "**EXPRESS: Cybercrimes Act Barometer**" no later than 24 November 2026 at 23:59 GMT+1.

Emails not so addressed will not be opened.