AVOCATS SANS FRONTIÈRES FRANCE

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

Call for Tenders: assessment of the implementation of the Cybercrimes Act in Nigeria and its implications for human rights

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
Duration	50 days
Project start and end dates	14 December 2026 – 15 April 2027
Deadline for submission of tenders	29 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 6

5. Expert profile 7

6. Budget, payment and contract terms 7

7. Evaluation of the tender 7

8. Intellectual property and confidentiality 7

9. Tender submission procedure 8

10. How to submit 8

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.

Alongside the Act exists a broader regulatory ecosystem encompassing data protection frameworks, electronic evidence rules, sectoral regulations, a national cybersecurity policy and strategy, and multiple enforcement and coordination bodies. However, operational implementation, judicial interpretation, human rights safeguards, and international cooperation across these areas have developed unevenly.

2. Purpose and Objectives of the Assignment

Rationale for the assignment.

Against this background, ASF France seeks an independent, evidence-based, and authoritative national study on the current implementation status and enforcement challenges of Nigeria's Cybercrimes Act.

Objectives

The **overall objective** of this call for tenders is to conduct a comprehensive national assessment of the implementation of Nigeria's Cybercrimes Act since 2015, identifying enforcement practices, institutional challenges and human rights implications, and developing practical recommendations to improve its effective and rights-compliant implementation.

Specific objectives:

1. Review the legal and institutional framework governing the implementation of the Cybercrimes Act, including its amendments, relevant regulations and related legislation.
2. Collect and analyse quantitative and qualitative data on the enforcement of the Act, including reported cases, investigations, prosecutions, convictions and the institutions involved.
3. Document and analyse cases involving the investigation, arrest, prosecution or conviction of human rights defenders, journalists, activists and civil society organisations under the Act, assessing their implications for freedom of expression, privacy, access to information and other fundamental rights.
4. Examine the use and potential misuse of the Act during election periods, identifying trends, risks and implications for civic space, democratic participation and fundamental freedoms.
5. Formulate evidence-based and actionable recommendations for legislative reform, institutional capacity-building and improved enforcement practices in line with international human rights standards.

Methodology

The consultant(s) will be expected to adopt a mixed-methods approach combining:

- **Desk review:** analysis of the Cybercrimes Act 2015, its 2024 amendment, relevant case law, regulations, national cybersecurity policies, institutional reports and relevant international human rights standards.
- **Quantitative research:** collection and analysis of available data on complaints, investigations, arrests, prosecutions and convictions under the Act, with particular attention to cases involving human rights defenders, journalists and activists.
- **Qualitative research:** semi-structured interviews with relevant stakeholders, including law enforcement agencies, judicial actors, lawyers, civil society organisations, journalists, digital rights experts and affected individuals.
- **Case studies:** documentation and analysis of selected cases illustrating the implementation of the Act and its implications for fundamental rights.

The proposed methodology must specify the sampling strategy, geographical coverage, target stakeholders, data collection tools and analytical framework. The consultant(s) must also

explain how the reliability of collected data will be ensured, particularly where official enforcement statistics are unavailable or incomplete.

3. Timetable

This study will run from 14 December 2026 to 15 April 2027, with an estimated duration of 50 working days.

Below is an indicative timetable for the project:

Phase	Timeline
Launch of the call for tenders	10 November 2026
Deadline for applications	29 November 2026
Start of the assignment	14 December 2026
Workshop to present the draft report	20 March 2027
Approval of the final report	29 March 2027
Webinar	Early 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

An **inception Report**, which is a refined and clarified version of the technical proposal for the planned mission. It must be submitted following the phase involving a review of the literature and the recontextualisation of the study. It must clarify the understanding of the assignment, the methodological approach – including sampling, the distribution and scheduling of interviews and focus groups – as well as the data collection and analysis tools, including questionnaires and an analysis plan. This kick-off report will be discussed and approved at a meeting between the consultant and ASF France in December 2026.

A **draft national assessment report** on the study, which will be submitted at the end of the analysis phase and presented during a provisional feedback workshop organised specifically for this purpose, in order to gather comments and encourage stakeholders to take ownership of the conclusions.

A **definitive final national assessment report** on the study, incorporating the feedback provided during the workshop, must be available within 7 working days of receipt of the comments. The report must clearly and unambiguously set out the analysis of the implementation of the Cybercrimes Act since its entry into force and its impact on human rights defenders. The final report will be presented during a webinar in April 2027.

A **four-page policy brief** must be produced to present the study's main findings and recommendation in an accessible manner. It will serve as an advocacy tool for institutional stakeholders and for dissemination to a wider audience.

The **slide presentation (PowerPoint) or visual aid** used to present the study's findings during the webinar must be shared with ASF France at least two days before the event.

5. Expert profile

The expert(s) must have the following qualifications:

- Advanced university degree (Master's or PhD) in law.
- At least 10 years of professional experience in cyber law, technology law, or cybersecurity policy.
- Demonstrated experience in conducting national research studies and producing evidence-based policy recommendations.
- Proven experience in qualitative and quantitative research methods, including interviews, case documentation and data analysis.
- Evidence of work involving Nigerian cybercrime, cybersecurity, or data protection law (research, legal practice, policy advice, or training)
- Certification in privacy, data protection, or cybersecurity is a plus.
- Experience in human rights analysis of digital laws.
- Fluency in written and spoken English.

6. Budget, payment and contract terms

The consultant(s) must submit a financial proposal and set it out in detail in the tender.

Payment shall be in instalments tied to progress of work. The final payment shall be made after the full report has been accepted.

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: assessment of the implementation of the Cybercrimes Act in Nigeria**" no later than 29 November 2026 at 23:59 GMT+1.

Emails not so addressed will not be opened.