

CYBERSECURITY AWARENESS CAMPAIGN AND TRAININGS

CONSULTANCY FIRMS REQUIRED

1. Background

The Private Sector and Innovation Promotion in Ghana (PSInno) project is part of the German Federal Ministry for Economic Cooperation and Development (BMZ) core theme, "Training and Sustainable Growth for Good Jobs in Ghana". The project is being implemented by Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH in collaboration with Ministry of Trade, Agribusiness and Industry. The objective of the project is to strengthen the competitive and employment-promotion economic development in selected sectors in Ghana, particularly in the north of the country.

PSInno supports growth-oriented small and medium-sized enterprises (SMEs) in Ghana with a focus on agribusiness, digital economy and innovation. Building on earlier private sector and entrepreneurship initiatives. In the agricultural and food sector, the programme targets producers, SMEs, and innovative enterprises in northern Ghana, whilst in the digital economy it targets all companies including startups and freelancers. PSInno works as a facilitator alongside business development service providers and financial institutions to improve market access, strengthen skills, and promote innovative business models. At the macro level, PSInno works with national and regional stakeholders to develop or reform policy instruments, contributing to an improved business environment for SMEs, while working with intermediaries to introduce new or adapted institutionalised support services to strengthen the competitiveness of companies in selected sectors.

2. Context of Consultancy

Ghana's digital economy is growing rapidly, creating new opportunities for SMEs across sectors. The adoption of digital tools and platforms, e-commerce channels, and mobile money services is increasingly essential to SME competitiveness, market access, and sustainable growth. However, increased digitalization also exposes businesses to a growing range of cyber threats, data breaches, online fraud, and mobile money scams- risks that many SMEs are poorly equipped to manage.

The Cyber Security Authority (CSA) is mandated to ensure cybersecurity regulation, coordination, and awareness in Ghana, while the Data Protection Commission (DPC) is the statutory body responsible for data protection regulation and the registration of data controllers and data processors in Ghana.

Several factors constrain SME market access and growth while undermining cybersecurity resilience and competitiveness in Ghana: low awareness and poor cyber hygiene, mobile money fraud, limited awareness of cybersecurity and data protection compliance pathways, and low levels of digital trust. These challenges are further compounded by the limited capacity of intermediary institutions, including innovation hubs, the Ghana Enterprises Agency (GEA), and sector associations, on which SMEs rely for business support. Many of these institutions do not yet offer cybersecurity or data protection advisory services as part of their existing SME services.

In response to these challenges, CSA, in collaboration with DPC, has requested support from the GIZ-implemented PSInno to position cybersecurity and data protection compliance as strategic drivers of SME competitiveness, scalability, and market readiness under the DigiShield Ghana initiative.

3. Objective of the Consultancy

The objective of this consultancy is to strengthen the cybersecurity and data protection resilience of growth-oriented SMEs in the Volta Region and build the capacity of selected intermediaries to provide sustainable advisory support to SMEs. The Volta Region will serve as a pilot for developing and validating an approach to inform the scale-up of DigiShield Ghana.

The specific objectives of this assignment are to:

- I. Establish a comprehensive evidence base on the cybersecurity and data protection needs, awareness levels, behavioural triggers and compliance gaps of participating SMEs and intermediaries in the Volta Region and map the relevant stakeholder landscape to inform targeted and context-specific programme engagement.
- II. Support CSA and partners to co-develop a practical, contextually relevant, and institutionally validated training package covering cybersecurity fundamentals, data protection and DPC compliance, mobile money fraud prevention, and digital safety, tailored to the distinct needs and roles of SMEs and intermediary organisations.
- III. Co-design and implement a coordinated DigiShield Ghana awareness and media campaign to strengthen cybersecurity and data protection awareness and promote behavioural change among SMEs, intermediaries, and business support actors.
- IV. Deliver practical cybersecurity and digital safety training to growth-oriented SMEs in the Volta Region and verify the adoption of safer digital practices among participants through structured post-training follow-up and behavioural assessment.

- V. Build and institutionalise cybersecurity and data protection advisory capacity in selected intermediary organisations, equipping 15 intermediary staff with the training, tools, and referral pathways needed to independently support SMEs beyond the life of the intervention.

- VI. Consolidate implementation results, document lessons learned and produce actionable recommendations to inform the scale-up of DigiShield Ghana to Northern Ghana and beyond.

4. Experience and Qualification Requirements

The assignment will be delivered by a two-person expert team comprising a Team Leader/Cybersecurity and Capacity-Building Expert and a Communications and Media Expert. The team should collectively demonstrate the following qualifications and experience:

Team Leader/Cybersecurity and Capacity-Building Expert

- Master's degree or equivalent in cybersecurity, IT, computer science, digital technology, information systems, project management, or a related field; relevant professional certifications are an advantage.
- Minimum 10 years of general professional experience, including at least 3–5 years in cybersecurity, digital safety, ICT, capacity building, or SME/private-sector support, and 5 years of team leadership or management experience.
- Demonstrated expertise in cybersecurity and data protection for SMEs, private-sector organisations, hubs, or intermediaries, including experience conducting needs assessments, stakeholder consultations, training, and capacity building.
- Demonstrated experience applying behavioural approaches to promote sustained adoption of safer digital practices, and experience translating assessment findings into practical interventions and recommendations.
- Strong knowledge of Ghana's SME, cybersecurity and data protection ecosystem, with at least 5 years of professional experience in Ghana. Experience in the Volta Region is an advantage.
- Strong experience in developing and delivering practical training, advisory tools, and institutional capacity-building interventions, including monitoring behavioural adoption and documenting lessons learned.

Communications and Media Expert

- University degree in communications, marketing, media studies, public relations, or a related field, with at least 5 years of professional experience in communications, media, public awareness, or marketing.
- Demonstrated experience designing and implementing multi-channel awareness campaigns across radio, print, digital and social media, including content development, media coordination, translation and localisation. Experience in cybersecurity or digital safety is an advantage.
- Experience supporting or co-facilitating training and capacity-building activities, preferably in Ghana, with familiarity with the Ghanaian media landscape.
- Fluency in English is required for both experts; proficiency in Ewe is a significant advantage. For the Communications Expert, proficiency in Twi is also desirable given the planned localisation of campaign materials.
- Strong facilitation, communication, analytical, creative, reporting and stakeholder-management skills are required across the team.
- Previous experience in GIZ or similar donor-funded/development cooperation projects is an advantage, with familiarity with GIZ project environments considered a significant asset.

Duration and Level of Effort

Period of assignment: 30th November 2026 to 30th July 2027 (9 months), comprising a total of 50 expert-days shared between two experts.

5. How to apply

Interested **consultancy firms** with proven experience in this area of work are kindly requested to express their interest in the above-mentioned assignment. Please send a Letter of Interest (LoI) with the following documents:

- Official letter expressing interest
- Profile of the firm and CV or portfolio of the proposed team (indicating relevant experience and qualifications)

- Proof of registration as a company
- Tax clearance certificate
- SSNIT certificate
- Any other relevant supporting document

How to apply

Please submit an expression of interest as indicated below, in **three separate folders as below**.

A. Commercial Folder

Please send the following documents:

- ❖ Official Letter of Expression of Interest
- ❖ Company profile
- ❖ Tax Clearance Certificate
- ❖ Business Registration Certificate
- ❖ Declaration of Business Ownership by General Manager (Inclusion of Form A for Sole Proprietorship or Form 3 for Limited Liability)
- ❖ VAT Registration Certificate
- ❖ SSNIT Clearance Certificate
- ❖ Other relevant supporting documents

B. Technical Folder

- ❖ Technical Proposal & CV/portfolio of the consultants (indicating the relevant experience and qualifications)

C. Financial Folder

- ❖ Financial offer

**PLEASE NOTE: THE CURRENCY OF YOUR OFFER SHOULD BE IN GHANA CEDIS
ALL PROSPECTIVE BIDDERS ARE REQUIRED TO PERFORM THEIR TAX
OBLIGATIONS IN GHANA.**

NOTE: Kindly visit the link below for **Terms of Reference** and **other documents** to be used in preparing your Technical and Financial Proposals

<https://www.giz.de/en/regions/africa/ghana/tenders>

Tender documents should be named according to the above in their respective folders (A- Commercial Qualification, B- Technical Proposal & CV/portfolio, and C- Financial Proposal) **and put into another folder and ZIP folder named as:**

"Expression of Interest for 10058599 / G-018082-001 / Cybersecurity Awareness Campaign and Trainings."

This tender will be accepted **ONLY** via email (**gh_quotation@giz.de**)

- **Tender Number must be used as the email Subject**
- **Please note that failure to comply with the above instructions, as well as submission to other e-mail addresses than the one mentioned, will lead to the disqualification of the bid.**

Bidding Conditions to all Bidders

- The deadline for submission is **06.11.2026 until 11:59 PM.**
- GIZ is not responsible for the failure of electronic delivery of e-mail messages to the address provided, whether due to technological problems on the part of GIZ or the applicant.
- This invitation to tender does not bind GIZ in any way. The contractual obligation of GIZ only begins with the signing of the contract with the successful bidder. Until the contract is signed, GIZ may either abandon or cancel the award procedure, without the candidates or bidders being entitled to claim any compensation.
- All costs associated with the preparation and submission of bidders are to be borne by the bidders and cannot be reimbursed.
- Financial bids should be valid for a period of three months from the date of submission.
- Please consider your bid unsuccessful if you do not hear from us after four weeks from the deadline of submission.

"Please note that participating in a tendering process of GIZ is free of charge for bidders.

At no phase of the process is the bidder required to make any payment to GIZ or to one of its employees.

Kindly Note by sending in your offer, you are agreeing to the GIZ General Terms and giving us the consent to process your company data.

ONLY SHORTLISTED FIRMS WILL BE CONTACTED