#ACT VBG

APPEL D'OFFRE CONSULTANT

Formation en sécurité numérique des ONG

PROFILS

Avoir une expérience en lien avec les objectifs de la recherche

OFFRE FINANCIÈRE

N'excède pas 300.000 FCFA

Le dépôt se fait entièrement par mail : princesseapinda@gmail.com et boussougouerisia7@gmail.com

Date limite de soumission des dossiers de subvention

au plus tard 23 juillet 2026 à 17h00

PARTENAIRES FINANCIERS

Cofinancé par l'Union européenne

AMBASSADE DE FRANCE AU GABON ET À SAO TOMÉ-ET-PRINCIPE

1. Contexte et justification

La lutte contre les violences basées sur le genre (VBG), en particulier celles exercées à l'encontre des femmes et des filles, constitue un enjeu majeur de protection des droits humains. Les organisations de la société civile engagées dans ce domaine collectent, traitent et conservent quotidiennement des informations sensibles concernant les survivantes, les témoins, les partenaires institutionnels ainsi que leurs propres équipes.

Dans un contexte de transformation numérique croissante, les organisations sont également confrontées à des risques nouveaux : cyberattaques, piratage des comptes professionnels, perte ou divulgation accidentelle de données confidentielles, usurpation d'identité numérique, hameçonnage (phishing), ou encore mauvaise gestion des systèmes de stockage des
informations.

Le projet Agir Contre toutes les formes de Violences Basées sur le Genre (ACT-VBG), financé par l'Union européenne ainsi que par l'Ambassade de France au Gabon à travers le Fonds Équipe France (FEF), est mis en œuvre par un consortium composé du Réseau Femme Lève-Toi (ReFLeT), d'Agir Ensemble pour les Droits Humains et d'Initiative Développement.

Téléphone : 077 95 69 69
Adresse : Ancienne sobraga
Plus d'informations citoyennes-engagees.org
@ACT VBG

AGIR ENSEMBLE POUR LES DROITS HUMAINS

Initiative Développement

AMBASSADE DE FRANCE AU GABON ET À SAO TOMÉ-ET-PRINCIPE

Cofinancé par l'Union européenne

Dans le cadre de son volet consacré au renforcement organisationnel, le projet prévoit des formations destinées à améliorer les capacités techniques et institutionnelles du ReFLeT afin de renforcer sa gouvernance, son efficacité opérationnelle et sa résilience organisationnelle.

La sécurité numérique constitue aujourd'hui un enjeu stratégique pour toute organisation œuvrant dans les domaines des droits humains, de la protection des victimes et du plaidoyer. Elle contribue non seulement à protéger les informations sensibles, mais également à garantir la confidentialité des données des bénéficiaires, la continuité des activités et la crédibilité de l'organisation auprès de ses partenaires techniques et financiers.

C'est dans cette perspective que le consortium souhaite recruter un(e) consultant(e) chargé(e) d'animer une formation en sécurité numérique adaptée aux réalités des organisations de la société civile.

2. Objectif

2.1 Objectif général

Renforcer les capacités des membres du ReFLeT en matière de sécurité numérique afin d'améliorer la protection des données, de prévenir les risques cybernétiques et d'adopter des pratiques numériques sûres dans la gestion quotidienne des activités de l'association.

2.2 Objectifs spécifiques

À l'issue de la formation, les participants devront être capables de :

1. Comprendre les enjeux de la sécurité numérique

- Comprendre les principaux risques numériques auxquels sont confrontées les ONG.

- Identifier les cybermenaces les plus fréquentes (phishing, malware, piratage, ingénierie sociale, etc.).
- Comprendre les conséquences d'une fuite de données pour les bénéficiaires et l'organisation.

2. Sécuriser les outils numériques

- Mettre en place des mots de passe robustes.
- Utiliser un gestionnaire de mots de passe.
- Activer la double authentification (2FA).
- Sécuriser les comptes Google, Microsoft, Facebook, WhatsApp et autres outils collaboratifs.

3. Protéger les données de l'organisation

- Organiser et classer les données sensibles.
- Sécuriser les espaces de stockage (Google Drive, OneDrive, Dropbox...).
- Mettre en place une politique de sauvegarde.
- Gérer les droits d'accès aux documents.

4. Adopter de bonnes pratiques numériques

- Sécuriser les ordinateurs et téléphones professionnels.
- Identifier les tentatives de fraude en ligne.
- Naviguer sur Internet en toute sécurité.
- Réagir efficacement en cas d'incident de sécurité.

5. Développer une culture de cybersécurité

- Élaborer des règles internes de sécurité numérique.
- Promouvoir les bonnes pratiques auprès des salariés, bénévoles et partenaires.
- Être capable de sensibiliser d'autres membres de l'organisation.

3. Mission et responsabilités

Sous la supervision de la Coordinatrice du projet ACT-VBG, le/la consultant(e) sera chargé(e) de :

- Concevoir le programme pédagogique de la formation ;
- Animer une formation participative auprès de 20 membres du ReFLeT ;
- Réaliser des exercices pratiques simulant des situations réelles ;
- Élaborer des recommandations adaptées aux pratiques du ReFLeT ;
- Évaluer les acquis des participants ;
- Produire un rapport final de formation.

4. Méthodologie

Le consultant devra privilégier une approche participative combinant théorie et pratique par des :

- exposés interactifs ;
- démonstrations pratiques ;
- études de cas adaptées au contexte des ONG ;
- simulations de cyberattaques (phishing, compromission de comptes, etc.) ;
- travaux de groupe ;
- exercices pratiques sur ordinateur et smartphone.

La formation devra être orientée vers des solutions simples, gratuites ou peu coûteuses, facilement mobilisables par une organisation de la société civile.

5. Livrables

Le consultant remettra :

- un programme détaillé de formation ;
- les supports pédagogiques ;
- les outils utilisés pendant les exercices pratiques ;
- des fiches de bonnes pratiques en sécurité numérique ;

- une proposition de guide ou de politique interne de sécurité numérique adaptée au ReFLeT ;

- un rapport de formation comprenant :
  - o le déroulement de la formation ;
  - o les résultats des évaluations pré et post-formation ;
  - o les recommandations pour renforcer durablement la sécurité numérique de l'organisation.

6. Profil, Qualification et compétences requises :

Le consultant devra justifier :

- d'un diplôme universitaire (Bac+2 minimum) en informatique, cybersécurité, systèmes d'information, protection des données ou domaine équivalent ;
- d'une expérience confirmée en cybersécurité ou sécurité numérique ;
- d'une expérience dans la formation des adultes ;
- d'une bonne connaissance des outils collaboratifs utilisés par les ONG (Google Workspace, Microsoft 365, plateformes collaboratives, etc.) ;
- une expérience auprès d'organisations de la société civile, de défense des droits humains ou d'organisations humanitaires constituera un atout.

7. Composition du dossier

Le dossier de candidature devra comprendre :

- une offre technique comprenant :
  - o la compréhension des présents termes de référence ;
  - o la méthodologie proposée ;
  - o le programme prévisionnel de formation ;
  - o le calendrier d'exécution ;

- une offre financière détaillée (en FCFA et en euros) qui n'excède pas 300.000 FCFA, incluant la taxe sur les prestations de service (TPS) pour 2 ou 3 jours de formation.
- un curriculum vitae détaillé détaillé présentant les références et les expériences en rapport avec l'objet de la mission;

8. Comment postuler

Pour postuler, les dossiers de candidature devront être transmis exclusivement par courrier électronique, avec pour objet : « ACT VBG – AO Formation en sécurité numérique », au plus tard 23 juillet 2026 à 17h00, aux adresses suivantes : princesseapinda@gmail.com et boussougouerisia7@gmail.com .

Pour toute demande d'informations complémentaires relatives au présent appel d'offres, les candidats peuvent contacter l'équipe projet aux numéros suivants : (+241) 074 44 98 66

Les candidatures reçues après cette date ou incomplètes ne seront pas examinées. Seuls les candidats présélectionnés seront contactés pour la suite du processus. ReFLeT se réserve le droit de ne pas donner suite au présent appel d'offres si aucune candidature ne répond aux exigences requises ou est incomplète.