Eviter la fraude et les irrégularités

1. Messages clés

Document de référence: Conditions Générales de la Convention de subvention – article II.16.2: https://ec.europa.eu/programmes/erasmus-plus/sites/default/files/2020-general-conditions-multibeneficiary_en.pdf

L'Agence **AEF Europe** applique une politique de tolérance zéro à la fraude

- L'AEF met en œuvre des mesures proactives pour :
  - Détecter, gérer les fraudes et prévenir tout risques d'occurrences
  - Engager des poursuites et récupérer les fonds
  - Rendre compte auprès de la Commission européenne
  - S'engage à respecter la confidentialité liée à l'investigation

En cas de suspicion de fraude, nous informer par email à:
partenariat@aef-europe.be

Toute plainte adressée à l'Agence sera examinée et fera l'objet d'une réponse.

2. Définitions

Irrégularité

Toute violation d'une disposition du droit communautaire ou toute inexécution d'une obligation contractuelle résultant d'un acte ou d'une omission d'un opérateur économique, qui a ou aurait pour effet de porter préjudice, par une dépense indue, au budget général des Communautés européennes ou à des budgets gérés par celles-ci.

! ≠ petite erreur administrative (petites erreurs de calcul/ de forfait, petites incompréhensions)

Fraude

Acte ou omission **intentionnelle** ayant pour résultat une baisse des revenus de l'UE ou un détournement des fonds. Le concept de fraude couvre une large palette d'irrégularités et d'actes illégaux caractérisés par une volonté de tromperie ou une déclaration mensongère avec pour conséquence une atteinte aux intérêts de l'UE.

Quelques exemples de fraude

Fraudes sur les dépenses / Recettes

- Déclarations/documents **faux, inexacts ou incomplets**
- **Non-communication** d'une information en violation d'une obligation spécifique
- **Détournement** de fonds européens à d'autres fins
- **Détournement** d'un avantage obtenu légalement

Effet

- Perception ou rétention indue de fonds européens
- Diminution illégale du budget européen

Corruption

- **Active**: action délibérée de solliciter ou recevoir un avantage pour accomplir ou non un acte dans l'exercice des fonctions professionnelles
- **Passive**: action délibérée de promettre ou donner un avantage à autrui pour accomplir ou non un acte dans l'exercice des fonctions professionnelles

3. Consignes de sécurité informatique (1)

Consulter régulièrement le site web https://www.safeonweb.be/fr ➡ information sur les risques actuels + conseils à appliquer

Processus liés aux paiements	Mettre en place des procédures, des règles de séparation de fonctions et de double signature.
	Sensibiliser les collaborateurs au phishing
	Toujours vérifier l'identité des titulaires des comptes bancaires
	Confirmer, par un échange téléphonique, les comptes bancaires
	Le compte bancaire doit être dans le pays du partenaire
	Prendre contact avec sa banque dès que possible en cas de doute ou si une erreur a été commise

4. Consignes de sécurité informatique (2)

En général	Sensibiliser les collaborateurs (notamment au phishing et à l'utilisation des données)
	Définir un plan de sécurité
	Installer un Antivirus sur tous les ordinateurs, tablettes, smartphone,….
	Installer un Firewall
	Maintenir les équipements informatiques à jour
	Veiller sur les vulnérabilités (outil de scan)
	Maîtriser les postes de travail : pas d'administrateur local parmi les agents
	Etablir et mettre à jour un inventaire des équipements et cartographie du réseau, bases de données, serveurs, etc.
	Etablir un inventaire des données critiques (RGPD) - gestion des actifs
	Mettre en place une politique de mots de passe et usage de l'informatique dans l'organisation (règlement de travail, charte utilisateur)
	Définir des droits d'accès minimum au données (sur le principe du "besoin d'en connaître" et du "moindre privilège")
	Contrôler les accès internet et WIFI
	Gérer les sauvegardes